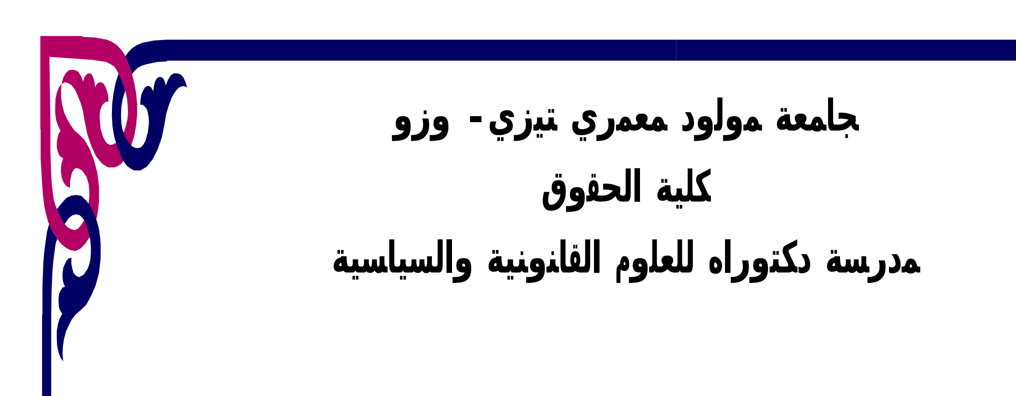
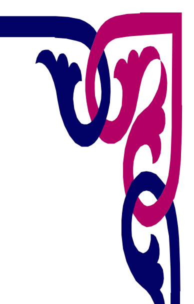




جامعة مولود معمري تيزي- وزو

كلية الحقوق

مدرسة دكتوراه للعلوم القانونية والسياسية

النظام القانوني للدفع الالكتروني

مذكرة لنيل درجة ماجستـ   القانون

فرع: القانون العام

صص:قانون التعاون الدو

إعـداد الطالب:

واقـد يوسف

تحت إشـراف:

الأستاذ: كاشير عبد القادر

<u>لجنة المناقشة:</u>

د.اقلولي محمد...........أستاذ محاضر (أ) جامعة تيزي وزو.....رئيسـ ـ ـ ـ ـ ـا

د.كاشير عبد القادر......أستاذ جامعة تيزي وزو...................مشرفا ومقررا

د.بوتوشنت عبد النور....أستاذ محاضر (أ) جامعة تيزي وزو......ممتحنـ ـ ـ ـ ـا

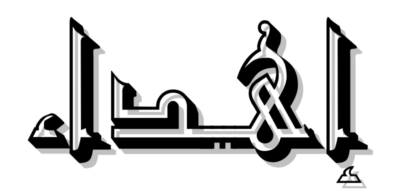
د.يسعد حورية...........أستاذة محاضرة (ب) جامعة تيزي وزو...ممتحنـ ـ ـ ـ ـا

تاريخ المناقشة: 2011/05/09



....وما توفيقي إلاّ با عليه توكلت وإليه أنيب

(سورة هود، الآية 88)





روح أ الطاهرة ر ة ا عليه

إ النور الذي أستضيء به طريقي هذه الدنيا أمي الغالية....

إخو العزيزات وإخوا الأعزاء....

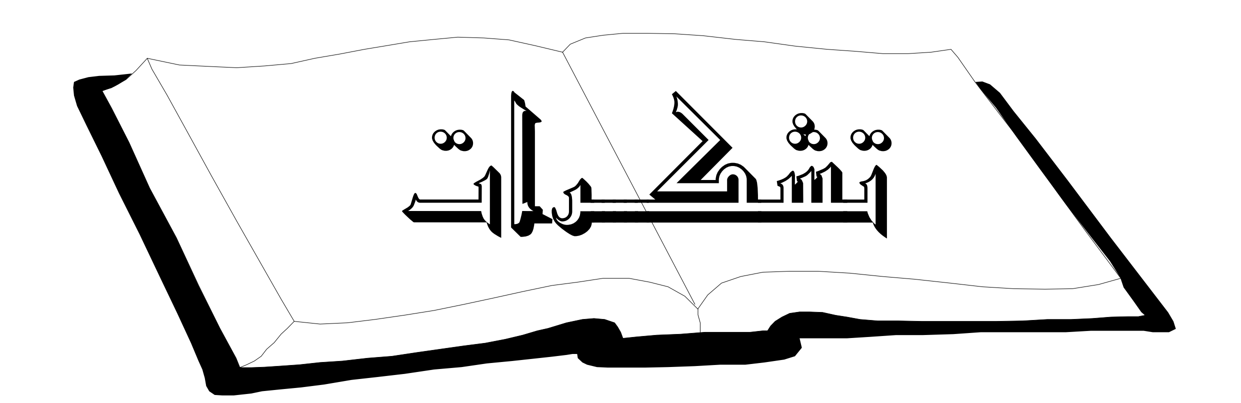
إ الكتاكيت ياس ، حس وأ د

وإ كل من خص بدعاء لص من القلب، وكل من شجع

إ از هذه ا ذكرة

وإ كل طالب علم

✍ **يوسف**



اعترافا بالفضل وا ميل أتوجه الص الشكر وعميق التقدير والامتنان إ

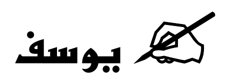
الأستاذ: كاش عبد القادر

الذي أشرف على هذا العمل، وتعهده بالتصويب يع مراحل إ ازه،

وزود بالنصائح والإرشادات ال أضاءت أمامي سبيل البحث.

كما أتقدم زيل الشكر إ كل من ساعد من بعيد أو من قريب

إ از هذا العمل ا تواضع .



بعض المختصرات

Liste des principales abréviations utilisées

باللغة العربية

ج ر : الجريدة الرسمية

ص : صفحة

ص ص : من صفحة إلى صفحة

ط : طبعة

ل.أ..م.ت.د : لجنة الأمم المتحدة للتجارة الدولية

E-MONEY : **E**lectronic **M**oney النقود الإلكترونية
EFT : **E**lectronic **F**ound **T**ransfert التحويل الإلكتروني الأموال
B2B : **B**usiness to **B**usiness- بين وحدتي عمل (مؤسستين)
B2C : **b**usiness to **C**ustumer- بين وحدة عمل و مستهلك
C2C : **C**ustumer to **C**ustumer- بين مستهلك ومستهلك
G2C : **G**overnment to **C**ustumer - بين قطاع حكومي و مستهلك

E-FINANCE : **E**lectronic **F**inance- التمويل الإلكتروني وكل ما يتعلق بالبنوك الإلكترونية
FTP :**F**ound **T**ransfert **P**rotocol. بروتوكول نقل البيانات
NTCI : **N**ouvelles **T**echnologies de la **C**ommunication et de l'**I**nformation.
ABP : **A**ssociation des **B**anquiers **P**rofessionnels.
EMV : **E**uropay **M**astercard and **V**isacard.
DAB : **D**istributeur **A**utomatique de **B**illets.
GAB : **G**uichet **a**utomatique de **b**anque.
ISO : **I**nternational **O**rganisation for **S**tandardization.
PIN : **P**ersonal **I**dentification **N**umber.

RIM : **R**éseau **M**onétique **I**nterbancaire.

TPE : **T**erminal de **P**aiement **E**lectronique.

SATIM : **S**ociété d'**A**utomatisation des **T**ransactions **I**nterbancaires et **M**onétiques.

LCR : **L**ettre de **C**hange **R**elevé (Papier ou Magnétique).

BCE : La **B**anque **C**entrale **E**uropéenne.

OP.CIT : opus citatum, locution latine qui signifie : ouvrage précédemment cité.

Ibid. : même ouvrage..

PP : de **P**age a la **P**age..

OMC : **O**rganisation **M**ondiale du **C**ommerce

مقدمـ ـة:

اجتهدت الإنسانية قصد تحقيق التطور الاقتصادي عبر مراحل عديدة، ساعية في كل منها للتنظيم الأحسن لشؤونها بما يتلاءم مع متطلباتها وحاجياتها حسب مقتضيات كل مرحلة. ورغم تشكيلها لدول مستقلة بعضها عن البعض الآخر سواء من حيث الإقليم الجغرافي أو الهوية الوطنية، إلاّ أن ذلك لم يمنع التعاون الدولي بينها في المجال التجاري قصد تحقيق التطور الاقتصادي والاجتماعي لكل منها.

فاعتمد الفرد في بداية المبادلات التجارية على نظام "المقايضة" للحصول على ما لا يمكن أن يوفره لنفسه من منتجات، إذ يتم تبادل كمية سلعة بسلعة أخرى حسب الاتفاق.

وبعد تطور الفكر البشري وتقدمه العلمي، أحدثت المجتمعات وسيلة جديدة للتبادل التجاري الداخلي منه والخارجي ألا وهي النـ ـقود (القطع والأوراق النقدية) La Monnaie Fiduciaire، والتي تستعمل إلى يومنا هذا كوسيلة للدفع والوفاء في المعاملات التجارية سواء كان محلها تبادل السلع أو الخدمات أو مشاريع استثمارية.

ولأهميتها أصبحت النقود التي تمثل مقابل وفاء الشيء محل المعاملات التجارية عنصرا جوهريا فيها. ويتبين التفسير القانوني والاقتصادي لعنصر الثمن على أنّه «مركز أو نقطة تلاقي الاقتصاد والقانون في مجال العلاقات والمعاملات بين المتعاملين، خاصة الاقتصاديين منهم في مجال التجارة، فالثمن يبين ويكشف عن التصرف القانوني الذي يكون عنصرا مهما في العملية أو الصفقة التجارية والذي يجعل من العقد قائما أو ممكن الوجود»[(1)].

1- **عبد الكريم موكه**، الثمن في عقود التجارة الدولية، مذكرة لنيل درجة ماجستير في القانون، فرع قانون الأعمال جامعة مولود معمري، تيزي وزو، 2007، ص17.

يعتبر ثمن السلعة أو الخدمة من بين الالتزامات الرئيسية والأساسية للمشتري[1] أو ملتقي الخدمة، الشيء الذي يدفعنا إلى ضرورة الاهتمام به وبكيفية انتقاله خاصة بعد ظهور البنوك كمؤسسات تجارية تتعامل بهذه الوسيلة وتنظم المعاملات ما بين المتعاملين، والتي تعتبر كوسيط تضفي صبغة الأمان والاحترافية على المعاملات النقدية فهي لا تقتصر على عمليات التوفير وتقديم الفوائد فقط، بل أصبحت تسهل انتقال الأموال مما يحفز توسيع نطاق المعاملات التجارية الالكترونية وتقوية الثقة فيها.

ومع ظهور تكنولوجيا الاتصال في ظل العولمة الرقمية، لم تبق تقنيات انتقال الأموال في منأى عن هذا التطور إذ مست كذلك خدمات البنوك وانتقال الأموال بالطرق المعلوماتية والرقمية لاتمام التزام الدفع.

نتج عن هذه الثورة العلمية شبكات اتصال عالمية، والتي يتم بموجبها تبادل المعلومات بين المتعاملين الاقتصاديين من أهمها الانترنت. تعتبر هذه الأخيرة نقطة تلاقي المنتجون والموزعون والبائعين وأصحاب الخدمات المختلفة قصد ربح الوقت وتقليص المسافات الجغرافية، فيتصل المتعاملين فيما بينهم عن طريق عناوين الكترونية خاصة بهم، فتحقق هذه وسيلة السرعة قدر كبير من الأمان في التجارة الإلكترونية.

تنقل شبكة الانترنت المعلومات التي تعبر عن إرادة المتعامل في اقتناء خدمات أو منتجات. فتؤدي هذه الطريقة المستحدثة في إبرام التصرفات القانونية إلى تلبية رغبات الشركات والمستهلكين على حد سواء، وذلك في خفض تكلفة السلعة أو الخدمة والرفع من كفاءتها ونجاعتها الاقتصادية لسرعة العمل بالطرق الرقمية وهذا ما يمسى بالتجارة الالكترونية.

1 - Deux obligations principales sont à la charge de l'acheteur, celle de payer le prix et celle de prendre livraison (le retirement) de la marchandise vendue. Le prix a été défini comme la contrepartie monétaire que l'acquéreur a l'obligation de payer au vendeur en contrepartie du transfert du droit de propriété. Sa présence est indispensable quant à la qualification du contrat de vente. Voir: **Houria YESSAD**, le contrat de vente internationale de marchandises, thèse pour le doctorat en droit, Université Mouloud Mammeri de Tizi-Ouzou, 2008, p315.

تتم التجارة الإلكترونية في سوق إلكتروني يتواصل فيه البائعون والوسطاء والمشترون، إذ تعرض فيه مختلف المنتجات والخدمات في صيغة افتراضية أو رقمية ويدفع ثمنها بالنقود الإلكترونية[1]، خاصة بعدما تم وضع برامج وتقنيات تهدف أساسا إلى ضمان حماية هذه المعاملات من كل الأساليب الإجرامية التي قد تتعرض لها.

فقد تم اختراع النقود الالكترونية وسائل عديدة لإتمام الدفع الالكتروني نذكر منها الشيك الالكتروني، والبطاقة البنكية وغيرها، والتي يتم التعامل بها بالطرق الرقمية عبر الشبكة العنكبوتية. لا يقتصر نطاق هذه الأخيرة في الحدود الجغرافية التقليدية بل يمتد ليشمل كافة المتعاملين أينما وجدوا في مختلف أنحاء العالم.

ومن أجل تطوير السوق النقدية والمصرفية، قامت الكثير من البنوك والمصارف بورشات عمل ضخمة ودراسات لتنظيم وتطوير أعمال الصيرفة الالكترونية بوسائل تقنية. كما يتطلب تحقيق هذا الهدف، إصدار العديد من القوانين والتنظيمات المبنية بدورها على دراسات قانونية دقيقة، سواء على المستوى الداخلي أو الإقليمي أو الدولي قصد تسهيل القيام بعمليات الدفع مباشرة عبر الشبكة العنكبوتية.

قصد تطوير استعمال البطاقات البنكية والأوراق التجارية المعالجة إلكترونيا وأنظمة الحواسيب لإتمام الالتزام بالدفع وتأمينه من الاعتداءات الرقمية حتى ينتج الآثار القانونية المرجوة من طرف المتعاملين. ونظرا للمخاطر التي تحمل التقنية الرقمية في طياتها من قرصنة المعلومات، والاختراقات والاعتداءات على المعلومات الشخصية وجدت عدة برامج الكترونية لوضع حد لمثل هذه الأساليب الإجرامية.

ومن أجل تحقيق هذا الغرض، اعتمدت الشركات العاملة في مجال تكنولوجيا المعلومات برامجا الكترونية قصد بعث الثقة بين المتعاملين وتطوير التجارة الالكترونية. وتعتبر هذه البرامج بمثابة نظم خاصة لحماية المواقع التجارية للشركات في شبكة الانترنت خاصة وأن المعاملات تتسم بطابع غير مادي بغياب السند الورقي فيها.

---

1 - **أمال حابت**، استغلال خدمات الانترنت، مذكرة لنيل درجة ماجستير في الحقوق، فرع قانون الأعمال، جامعة مولود معمري، تيزي وزو، 2004، ص20 .

فكلما وفّر الموقع الالكتروني حماية فعالة كلما حصلت الشركة التجارية صاحبة هذا الموقع إقبالا ملحوظا من المتعاملين، وسجلت أرباحا ضخمة مما يعكس الأهمية البالغة للتجارة الالكترونية.

وبتعبير آخر، يرجح الكثير من الاقتصاديين أن التجارة الالكترونية مجال للنمو الضخم، فيتم يوميا تحصيل وصرف مبالغ معتبرة بمناسبة المعاملات التجارية الالكترونية. إذ يكفي أن نعرف أن ملايين الأفراد حول العالم يستعملون هذه الخدمات لندرك قيمة هذه المتطلبات وأهميتها، وذلك راجع إلى انخفاض نفقات التعامل التجاري وتنوع الأسواق على الانترنت، الشيء الذي يمكننا بمقارنة الأسعار التي تقدمها الشركات عبر الانترنت للمستهلك.

ولاختيار بين أفضل مقدم لخدمة الدفع الالكتروني من بين البنوك التي تتدخل في عملية الاقتناء ولذلك تعتبر من العناصر الأساسية لبحثنا والتي تتعامل أساسا بالتحويل الالكتروني للأموال (electronic fund transfer).

واستجابة لهذه المتطلبات ظهرت البنوك الالكترونية أو البنوك على الخط لتسهيل المعاملات المصرفية مسايرة بصفة كبيرة لبيئة التجارة الالكترونية، التي تتعامل مع كافة المتعاملين الاقتصاديين من تجار وموردين وبائعين والتي تعمل على تسيير حساباتهم عبر الخط مباشرة.

فوفرت المؤسسات المؤسسات المصرفية خدمات عبر الانترنت قصد تحقيق أهداف مختلف المتدخلين اعتمادا على وسائل قانونية وتقنية منها بطاقات بنكية، وأوراق تجارية مرقمة، المجردة من الطابع المادي مقارنة بالوسائل الكلاسيكية عدا البطاقة البنكية التي تتمتع بطابع مادي إلا أن حمولتها تتجرد من هذه الطبيعة، فمعظم الخدمات المقدمة على شبكة الانترنت تقبل الدفع بواسطة هذه الوسائل خاصة وأن الأوضاع الاقتصادية والتطورات التجارية العالمية أصبحت تفرض التعامل بهذه الطرق على الخط.

ولكن لم تحمل التكنولوجية المعلوماتية إيجابيات ومحاسن فقط بل حملت أيضا خطر التعرض غير المشروع للبيانات بالاعتداء عليها عن طريق القرصنة، السرقة

والتزوير على الخط التي عرفت صدى كبير خاصة الاعتداء على أرقام البطاقات البنكية وتغيير بيانات الرسائل الإلكترونية فأصبحت هذه التقنية شر لابد منه في ظل حتمية الاندماج في العولمة المفروضة.

كان من الضروري مواجهة هذه السلبيات بتوفير الوسائل القانونية والتقنية لضمان السير الحسن لمعاملات التجارة الإلكترونية ومجال المعلوماتية، من أجل تطويرها خاصة ما يتعلق بالدفع الالكتروني من خلال خلق الجو الملائم لإتمامها والاجتهاد مع مختلف المؤسسات من بنوك وجامعات ومختصين في الإعلام الآلي والبرمجيات قصد تطويره.

واستجابة لمبدأ السرعة والثقة التي ترتكز عليها التجارة بإصدار الكروت البنكية لمختلف شرائح المجتمع وتوزيع نهائيات الدفع وموزعي الأوراق النقدية قصد تحقيق نجاعة ومسايرة القوانين الدولية التي تسعى لتحقيق تعاون دولي متوازن القوى والفرص ووضع حد لتبعية وهيمنة دولة لدولة أخرى في مجال التجارة الالكترونية بالهوة في التقدم التكنولوجي بينها.

أصبحت التجارة الإلكترونية مركز اهتمام كافة الدول والمنظمات الدولية وعلى رأسها المنظمة العالمية للتجارة التي اعتبرتها من بين أهدافها التي تسعى إلى تطويرها.

كما يظهر التعاون الدولي لتنظيم والتحكم في الدفع الالكتروني، من خلال اهتمام المنظمات الدولية لهذه التقنية كالمنظمة العالمية للتجارة ولجنة التجارة الدولية التابعة لهيئة الأمم المتحدة والتي تهتم بالتجارة الالكترونية[1].

وكذا التجمعات الإقليمية كالاتحاد الأوروبي وذلك من خلال تنظيمها لهذه التقنية بقوانين وتشريعات تتعدى البعد الداخلي للدولة الواحدة وإصدارها توصيات قصد الاستفادة من خدمات الدفع الالكتروني والعمل على نشرها في كل إنحاء العالم.

كما ظهر في إفريقيا مشروع تطوير هذه الخدمات وذلك بالتعاون مع الاتحاد الدولي للبريد UPU والصندوق العالمي للتطوير الفلاحي، ومن خلال منظمة (OHADA)

1- **وثيقة لجنة الأمم المتحدة للقانون التجاري الدولي،** الفريق العامل المعني بالتجارة الالكترونية، الجوانب القانونية من التجارة الالكترونية، الدورة 38 نيويورك، من 12-23 مارس2001، ص3.

- **OHADA** : organisation pour l'harmonisation en Afrique du droit des affaires.in : http://fr.wikipedia.org

وذلك لتطوير استعمال تكنولوجيا الاتصالات وغيرها من المشاريع التي تسعى إلى تحقيق تعاون دولي في مجال ردع القرصنة الالكترونية وحماية الملكية الفكرية والكثير من الجوانب المتعلقة بتكنولوجيا الاتصال والإعلام وتطوير التجارة الالكترونية بصفة عامة والدفع الالكتروني الذي يمس بجوهر العلاقة ألا وهو الثمن أي مقابل السلعة أو الخدمة.

والجزائر لم تبقى في منأى عن هذه التطورات، فلقد لاحظنا في الآونة الأخيرة السماح للبنوك الخارجية ذات السمعة العالمية والتي تعمل بنظام الدفع الالكتروني بنسبة كبيرة في معاملاتها مثل BNP Paribas – Société Générale ...إلى آخره للدخول إلى السوق الوطنية وتقديم خدماتها.

مست هذه التوجهات الاقتصادية الجديدة استعمال تكنولوجيا الاتصالات النظام المصرفي الجزائري، كما عمدت البنوك الوطنية إلى الاستثمار في هذا المجال لتطوير خدماتها المصرفية لمواجهة المنافسة المحلية والدولية في هذا الميدان.

ففاق عدد الشركات التي ترغب في الاستثمار في هذا المجال عشرين شركة منذ سنة 2000، غير أن شركتين فقط فرضتا نفسيهما في السوق ويتعلق الأمر بـ **إيباد وجيكوس** خاصة وأن عدد الأنترناتيين عرف ارتفاع ملحوظ ، فهذا المعيار يمثل قاعدة التجارة الالكترونية بزيادة إسهامها في التجارة العالمية وكذلك لتطور قطاعاتها الإنتاجية الوطنية وإتاحة فرص لرفع معدلات نموها الاقتصادي.

وخلق جو من المنافسة المشروعة ما بين المؤسسات الصغيرة التي تنشط خاصة في مجال الاستيراد والتصدير، وذلك للسعي وراء الحصول على أكبر نسبة ممكنة من السوق في الوقت الذي تتفتح فيه شبكات الاتصالات على كافة الأسواق العالمية وإدماجها لمختلف النشاطات التجارية، والتي تتم في مجال التجارة الالكترونية والتعامل بمختلف جوانبه مثل الدفع الالكتروني.

وأصبح هدف هذه الدراسة إذن هو إبراز مختلف الجوانب الجوهرية (القانونية والتقنية) للدفع الالكتروني من حيث تنظيم التعامل به، وتسليط الضوء على الحماية من المخاطر التي يتعرض لها للأهمية الكبيرة التي يلعبها في التجارة الالكترونية وتزيد أهمية

الموضوع بعد تطور أحكام الوفاء والإثبات في البيئة الإلكترونية، ونرجو أن يكون هذا البحث لبنة في المكتبة القانونية.

ومن أجل ذلك ارتأينا إلى هذه الدراسة المتخصصة من خلال تحليل الإشكالية الآتية: **ما هو النظام القانوني الذي تمارس فيه تقنية الدفع الالكتروني وحمايتها في ظل تكنولوجيات الاتصالات الرقمية**؟ وللإجابة على هذه الإشكالية يقتضي منا الموضوع دراسة ماهية الدفع الالكتروني بإبراز عناصر تقنية الدفع الالكتروني (فصل أول).

ونظرا لتعرض الدفع الإلكتروني لعدة مخاطر الاعتداء عليه والتي تعتبر محل اهتمام مستعملي هذه التقنية، ارتأينا دراسة وتشخيص هذه الجرائم التي تعاني منها تقنيات المعاملات الإلكترونية ثم كيفية التصدي لها قصد تحقيق الضمان والأمان والسرعة التي تستوجبها الأعمال التجارية (فصل ثان).

الفصل الأول:

ماهية الدفع الالكترونية

لقد بلغ التقدم العلمي والتكنولوجي اللذين عرفهما العالم في منتصف القرن الماضي خاصة إلى أبعد الحدود خدمة للمجتمعات، واستجابة لحاجيات الفرد الذي يسعى إلى تسهيل وتفعيل نشاطاته الاقتصادية المتداخلة بعضها البعض من إنتاج، تسويق، توزيع وانتقال رؤوس أموال.

وحفزت ذلك شبكة اتصالات عالمية شاملة مابين المتعاملين، من مؤسسات مالية منتجين وموردين ومستهلكين، فاعتمدت شبكة الإنترنت العالمية على البيانات لتبادل المعلومات كوسيلة ذات طبيعة غير مادية ربحا للوقت وتقليصا لتكلفة المعاملات.

فاهتمت السياسات الداخلية للدول، وكذا المنشآت التجارية والمستهلكون في جميع أنحاء العالم بهذه الشبكة لما تقدمه من تسهيلات وخدمات تجارية جوهرية فأصبح الآن بإمكان أية منشاة تجارية رغم صغر حجمها أن تتحول إلى شركة عالمية بمجرد أن تنشئ لنفسها موقعا على الإنترنت[1].

كما تجدر الإشارة إلى أنّه لا تعتبرا لإنترنت الشريك الوحيد في مجال الدفع الإلكتروني وإنما هناك من ينادي بترقية الوسائل الأخرى مثل الأنترانت، الإكسترانت والهاتف النقال الذي يعد الوسيلة الأكثر تداولا لدى الأفراد، وهذا ما سعت إليه شركة (Tagattitude) التي تسعى إلى تطوير السوق الإفريقية في هذا المجال، حيث سعى مؤسسها إلى تطوير دفع وسحب الأموال بالهاتف النقال، خاصة في البلدان الأقل تطورا في استعمال تقنيات الدفع الالكتروني[2]، وهذا بالتعاون مع البنوك المحلية والمؤسسات الخاصة في هذا المجال.

مما يستوجب التعرف على هذه الشبكة التي توفر للبشرية إمكانيات تعامل هائلة في مجالات متعددة كالتسويق والتبادل التجاري، وكذلك الدفع الإلكتروني الذي يتم بواسطتها. لذا ارتأينا دراسة محتويات هذه التقنية بالتعريف وتحليل الدفع الإلكتروني في العالم الافتراضي (المبحث الأول).

1- **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2006، ص11.

2- **DESAVIE Patrick**, « avec tagattitude le téléphone paie », article du 23/01/2009 in: www.tagattitude.fr

كما تم استحداث وسائل عديدة يستخدمها المتعاملون قصد الوفاء بما اقتنوه من سلع وخدمات، وهي وسائل الدفع الإلكترونية التي تجد مجالا واسعا في جميع مجالات التجارة سواء التجارة التقليدية أو الإلكترونية[1]. إلاّ أنّها تجد هذه الوسائل مجالها الخصب في التجارة الإلكترونية والبنوك الإلكترونية على الخط[2].

وقد ارتأينا دراسة وسائل الدفع الإلكترونية التي يعتبر استعمالها ذات بعد داخلي وفي نفس الوقت عالمي، حيث تسعى الكثير من المؤسسات إلى تحديث تقنياتها ووضع برامج خاصة بهذه التقنية حيز التنفيذ، لكي تستعمل هذه البرامج لتقديم خدمات الدفع من طرف كل متعاملين المؤسسة نفسها عبر الإنترنت الشبكة المفتوحة على كل شخص بمجرد امتلاك موزع الاستعمال والربط بالشبكة للحصول على معلومات، والتي توفر طرق تعامل جديدة من خلالها، والتي تغطي الكثير من الدول المتباينة تشريعيا[3] (المبحث الثاني).

1- وتجدر الإشارة أنه ليس هناك ما يمنع من أن تتم الصفقة بطريقة تقليدية (غير الكترونية... ولكن يتم الوفاء بطريقة الكترونية). أنظر في ذلك: **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية وسائل الدفع الالكترونية الحديثة دار الفكر الجامعي، الإسكندرية، مصر، 2005، ص 324.

2- المرجع نفسه، ص324.

3 - **DAJO Cica Mathilda**, Les contrats dans le cyberespace à l'épreuve de la théorie générale, problèmes et perspectives, mémoire de Maîtrise en droit des affaires et carrières juridiques, Bénin Mémoire publié sur le site: www.memoireonline.com.

المبحث الأول

الدفع الإلكتروني في العالم الافتراضي

تعتبر شبكة الاتصالات العالمية "الإنترنت" البيئة التي تنمو فيها المعاملات الاقتصادية الحديثة عامة والدفع الإلكتروني على وجه الخصوص، فعرفت سرعة انتشار مذهلة حيث استغرقت فقط أربعة أعوام لكي يصل مستخدميها إلى خمسون مليون مستخدم[1]، بالاعتماد على برامج الحواسيب وتبادل البيانات التي ترسل عبر قنوات وعناوين إلكترونية يمتلكها كل متعامل على هذه الشبكة، مما يستدعي دراسة طرق الدفع الإلكتروني (مطلب أول).

كما أتت الانترنت بخصوصية جد مهمة في معاملاتها تتمثل في تجريد المعاملات من طبيعتها المادية على غرار المعاملات الكلاسيكية التي تتميز بها فيتم الاستغناء عن الورق(الدعائم الورقية)، الذي تتم بواسطته تحرير مختلف العقود التقليدية وتعويضه بالمعلومات والبيانات الإلكترونية مما يستدعي البحث حول طبيعة البيانات الالكترونية وحجيتها التي تتداول في ظل تكنولوجيا المعلومات باستعمال الحواسيب (الكمبيوتر) المتصلة بعضها البعض والتي يتم إرسال هذه المعلومات من خلالها مما يستدعي دراسة هذه البيانات والمعلومات في مجال الدفع الإلكتروني (مطلب ثاني).

---

1 - استغرق التليفون أربعة وسبعين عاما والتلفزيون 13عاما للوصول إلى هذا الرقم، ولقد سهلت تقنية الاتصالات خاصة بعد أن صممت شركة مايكروسوفت برنامج النوافذ وسهولة الاتصالات.أنظر: **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص11.

المطلب الأول
طرق الدفع الإلكترونية

تعتبر شبكة الاتصالات العالمية الانترنت المجال الخصب الشامل الذي تتداخل فيه كافة القنوات الإقليمية والداخلية المتصلة بعضها البعض، فتشكّل بذلك شبكة عالمية ضخمة الحجم والاستعمال، تتم عن طريقها عملية الدفع الإلكتروني (فرع أول) مما يسمح لنا بتقديم تعريف للدفع الإلكتروني بعد ذلك (فرع ثاني).

الفرع الأول
الاتصالات الإلكترونية

يعتبر المعنى الاصطلاحي لتقنية المعلومات "أحكام المعلومات من جهة سرعة الحفظ، وجودة التخزين وسرعة الوصول إلى المعلومات وسهولة التعامل معها وسهولة تبادل المعلومات بين المتعاملين بينهم.

أولا- تعريف الإنترنت

اصطلاح "الإنترنت" (Internet) هو اختصار لكلمتين انجليزيتين الأولى هي (International) والثانية (Network)، بالتالي هي كلمة مركبة سميت بها شبكة عنكبوتيه تتكون من الملايين من قنوات المعلوماتية المتصلة بعضها البعض، فيصعب إذن تحديد حجمها وكثافتها، والتي تستعمل الحواسيب لاقتناء أغراض المتعاملين وتصرفاتهم القانونية[1].

1 - **عبد الرحمن بن عبد ا السند**، الأحكام الفقهية للتعاملات الالكترونية (الحاسب الآلي وشبكة المعلومات "الانترنت"، دار الوراق للنشر والتوزيع، الرياض، 2004، ص20.

الانترنت هي الملايين من أجهزة الكمبيوتر المتصلة بعضها البعض، علي النحو يمكن لمستخدميها الوصول إلي المعلومات والمشاركة في الملفات. أنظر في نفس السياق: **محمد عبد حسين آل فرج الطائي**، المدخل إلى نظم المعلومات الإدارية، وائل للنشر والتوزيع، الطبعة الأولى، عمان، 2005، ص182.

كما تتميز الإنترنت بخصوصية إمكانية وجودها في عدة أماكن في نفس الوقت وهذا ما يسمى باللاتينية(*)L'ubiquité(1) فتتعدى المجال أو مفهوم الإقليم والجنسية التقليديين إلى المساس بكافة أنحاء العالم التي يمكن ربطها بها لذاك تسمى بالشبكة الأم.

وبالتالي توفر إمكانية الحصول على المعلومات في مختلف الدول في أن واحد وهذا ما دفع إلى تكييفها كذلك أنها مجردة من الإقليم الجغرافي باعتبارها متكونة من ملايين الشبكات الحرة وتعدد الموزعين الأصليين المكونين لها التي تسمح بنقل البيانات بمجرد الدخول إلى موقع المؤسسة والنقر على الخدمة أو السلعة التي يرغب في الحصول عليها. كما تعد هذه الملايين من الشبكات حرة بعضها البعض حيث أن عدم تشغيل أحدها لا يعطل استعمال الشبكات الأخرى(2).

ونتج عن ذلك شبكة الاتصالات الدولية ضخمة جدا ومن أهم التعريفات التي قدمت لها كذلك أنّها :«**شبكة هائلة من أجهزة الكمبيوتر المتصلة فيما بينها بواسطة خطوط الاتصال عبر العالم**»(3). فهو عبارة عن نظام نقل المعلومات فيمكن لأي شخص لديه جهاز الكمبيوتر مزود بجهاز المودم (Modem) ولديه اشتراك لدى أحد مقدمي خدمة الإنترنت الدخول على الإنترنت(4).

---

*- Ubiquité : en latin ubique (partout), attribue à dieu, présent partout dans un même instant. Possibilité d'être présent en plusieurs lieux à la fois.
- «Ubiquité ou avoir le don d'ubiquité c'est pouvoir être dans plusieurs endroit a la même fois ».

1- **Le Robert junior**, édition le Robert, Paris, 2005, p.1055 et voir aussi : **Le petit Robert1**, Edition le Robert, Paris, 1990, p2045.

2- En Afrique il y a au moins fournisseur d'accès par pays contre une centaine en France sans parler des fournisseurs d'accès américains et des fournisseurs d'accès en ligne. Voir : **DAJO Cica Mathilda**, Les contrats dans le cyberespace à l'épreuve de la théorie générale, problèmes et perspectives, op.cit, p.8 .

3-**Roger Loroy Miller et Gaylord A.Jentz**, Law for Electronic, commerce, Thomson, 2000, p.7.

4- ظهرت النواة الأولى لفكرة شبكة الانترنت في أواخر الستينات من القرن الماضي وبالتحديد عام 1969... وكان الدافع من هذه الشبكة تحقيق هدف استراتيجي وهو إرسال تعليمات التصويب من خلال مركز التحكم إلى قواعد الصواريخ... أنظر في ذلك: **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص12.

فتمكننا الشبكة العنكبوتية من إرسال واستقبال المعلومات من وإلى مختلف أجهزة الحواسيب نحو المواقع التي نختارها والتي نريد أن نتعامل مع أصحابها.

ثانيا- الإنترنت والتجارة الإلكترونية:

تعتبر شبكة الاتصالات العالمية "الإنترنت" البيئة التي ولدت فيها للتجارة الإلكترونية رغم وجود تباين في تعريف التجارة الإلكترونية.

فهناك فريق من الفقه يرى أن التجارة الإلكترونية هي التجارة التي تتم من خلال الإنترنت، وفريق آخر يرى أنها التجارة التي تتم من خلال أي وسيط الكتروني سواء تمثل ذلك على الإنترنت أو غيره من الوسائط الإلكترونية[1].

واعتمدت القواعد الصادرة عن لجنة القانون التجاري الدولي بالأمم المتحدة عام 1996(الأونسيترال) على المفهوم الواسع والتي تحدد في المادة الأولى منها نطاق تطبيق هذا القانون فينص «**ينطبق هذا القانون على أي نوع من المعلومات يكون على شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية»[2].**

فيعتمد على الإنترنت بشكل رئيسي في شتى أنواع التجارة الإلكترونية. بحسب أطرافها سواء كان بين وحدتي أعمال(B2B) أو بين وحدة أعمال ومستهلك (B2C) بين مستهلك ومستهلك (C2C) أو بين قطاع حكومي ومستهلك (G2C) .

فالأنترنت ساعدت كثيرا على ازدهار وتطور التجارة الإلكترونية وانتشار المنتجات والخدمات المالية مثل التأمين والسمسرة وظهور النقود الرقمية (Digital money) والدفع والتمويل الإلكتروني من طرف البنوك وهذا ما يسمى بـ (E-Finance) كتقنية تضمن جميع أنشطة التمويل التي يمكن تنفيذها من خلال شبكة الإنترنت[3].

1- **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية وسائل الدفع الالكترونية الحديثة، المرجع السابق ص325.

2- المادة الأولى من القانون النموذجي للاونيسترال بشأن التجارة الإلكترونية. ل. أ. م. ت.د، الجلسة العامة 85 المؤرخة في 16 ديسمبر 1996.

3- **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص15.

ثالثا-خدمات الكمبيوتر:

ساهم التطور التكنولوجي في مجال الاتصالات في دفع بالمتعاملين الاقتصاديين إلى استخدام العقـول الإلكترونية في كثيـر من نواحي النشـاطات الاقتصادية، وهو الشأن كذلك بالنسبـة للدفـع الإلكتروني، فتقوم المؤسسات المالية بتقديم هذه الخدمات مقابل عمولة تتحصل عليها[1].

وعلى سبيل المثال تنتظر البنوك في الولايات المتحدة الأمريكية أن تتزايد خدماتها للمتعاملين معها باستعمال الحاسب الإلكتروني تزايدا مهما في السنوات القليلة القادمة، حيث يصبح إيرادها في مثل هذه الخدمات في المرتبة الأولى ويطغى على الإيرادات من عمليات التسليف الكلاسيكية [2].

كما يتعهد نظام الشبكة العنكبوتية في إحداث ثورة في مجال التجارة الإلكترونية كما أشار إلى ذلك "Olivier Iteanu" أن التجارة الإلكترونية تظهر لنا تجارة كغيرها من ناحية المضمون والمتعاملين الذين يقومون بها، لكن طرق تنفيذها وتنفيذ عقودها تستأثر بها لوحدها، والتي تظهر مجال جديد للقانونيين فيما يخص طرق الدفع التي تعرض على الشبكة، وكذا دولية العلاقات والعراقيل المحتملة لاكتمال صفقة الكترونية معينة[3].

كنتيجة لذلك أصبحت الأنظمة المستعملة لمبادلة واستعمال وسائل الدفع بين البنوك مرقمة (numérisée)، ومؤمنة فيجب مراعاة قواعد استخدامها والاستفادة منها خاصة وأنّه قد تم تدويلها بعدما تضاعفت قنوات الاتصال بين البنوك وزبائنهم المتصلة بالإنترنت، كشبكات الهاتف (Suift net) رغم ما تحدث من إشكالية تطور البنوك

---

1 - **زياد سليم رمضان، محفوظ أحمد جورة**، الاتجاهات المعاصرة في إدارة البنوك، الطبعة الثانية، دار وائل للنشر والتوزيع، عمان، 2003، ص22.

2 - المرجع نفسه، ص22.

3- Internet promet de Bouleverser également l'organisation du commerce traditionnel si comme l'indique Me Olivier Iteanu, le commerce électronique semble bien un commerce comme les autres du point de vue de son contenu et des acteurs qui le pratiquent en revanche, ses modalité d'exécution , notamment le mode conclusion et l'exécution du contrat , apparaissent particulier. Voir: **TORTELLO Nicole**, **LOINTIER Pascal**, Internet pour les juristes, Dalloz, Paris, 1996, p22.

الإلكترونية التي تساهم في ربح المردودية للبنوك وتخصيب الخدمات للزبائن نجد في أوروبا مثلا دفع المبالغ الضخمة باليورو ومعالجة العمليات بنظام الكتروني عابر للحدود ومؤمن ضد المخاطر المعلوماتية المالية، مسير مباشرة من طرف البنك المركزي الأوربي باستعمال نظام (Target) الذي يعتبر ميكانيزم ضمان في إطار النظام المالي الأوربي (Euro system) في أوروبا[1].

أما في الجزائر فقد نص القانون على ترخيص تقديم خدمات أنترنات واستغلالها لأغراض تجارية وبشروط محددة مسبقا التي تتمثل في الأشخاص المعنويين الخاضعين للقانون الجزائري.

ويظهر ذلك من خلال المادة الرابعة من المرسوم التنفيذي 2000-307 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها والتي تنص «**لا يرخص بإقامة خدمات أنترنات واستغلالها لأغراض تجارية ضمن الشروط المحددة أدناه، إلاّ للأشخاص المعنويين الخاضعين للقانون الجزائري الذين يدعون أدناه مقدمي خدمات أنترنات**»[2].

رابعا- مزايا ووظائف الإنترنت في التجارة الالكترونية:

خلقت شبكة الإنترنت الجو الملائم الذي تمارس فيه التجارة الإلكترونية، لما توفره من مزايا عديدة ووظائف مهمة الشيء الذي دفع غالب التشريعات الداخلية للدول تنظيم الممارسات القائمة في ظل هذه الشبكة، فمزاياها كثيرة، ولا بأس ذكر البعض منها:

- قلة تكلفة عقد الصفقات التي تتم عبر شبكة الانترنت.
- التفتح على السوق العالمية دون حدود زمنية ولا مكانية.

1- **BOUYALA Régis**, Le monde des paiements , édition Revue banque , 2005, p.13.

2- راجع المادة الرابعة من المرسوم التنفيذي رقم 2000-307 مؤرخ في 16 رجب عام 1421 الموافق لـ 14 أكتوبر سنة 2000 يعدل المرسوم التنفيذي رقم 98-257 المؤرخ في 3 جمادي الأولى عام 1419 الموافق لـ 25 غشت سنة 1998 الذي يضبط شروط وكيفيات إقامة خدمات أنترنات واستغلالها ج.ر العدد15، 15 أكتوبر 2000.

- خلق أسواق جديدة باحتكاك مختلف المؤسسات والمتعاملين عبر الأسواق المفتوحة على الشبكة.[1]
- السرعة والفعالية في عقد الصفقات وتنفيذ العقود والتزامات الأطراف حيث يتم الدفع عن طريق إرسال مجموعة من البيانات الشخصية من المشتري إلى البائع قصد خصم قيمة الشيء أو الخدمة عن طريق الاتصالات.

خامسا- حكم استخدام الإنترنت في الشريعة الإسلامية:

اعتبرت الشريعة الإسلامية حكم استعمال الوسائل نفس حكم مقاصدها التي تؤدي إليها، وعلى ذلك فإذا أردنا أن نعرف حكم وسيلة ما نظرنا إلى المقصد الذي تؤدي إليه أو الذي يراد تحقيقه باستخدامها.

فإذا كان المقصد مباحا كانت الوسيلة مباحة وهكذا أي انه للوسائل أحكام المقاصد من الوجوب وعلى ذلك فإذا احل ا شيئا احل وسائله المؤدية إليه فالعبرة على مدى مشروعية الوسيلة في الفقه الإسلامي تنحصر في مدى مشروعية الهدف أو المقصد الذي يراد الوصول إليه بهذه الوسيلة.

وعلى ذلك فان استخدام الإنترنت في البيوع الإلكترونية المباحة شرعا هو أمر مشروع وجائز في الفقه الإسلامي، لأن الهدف أو المقصد مشروع وجائز كما بينا ذلك[2].

والشبكة التي يتم من خلالها الدفع الإلكتروني يمكن أن يكون الاتصال بها مقتصرا على أطراف التعاقد (Mono fournisseur) وهذا يقتصر في تواجد معاملات وعلاقات تجارية ومالية سلفا بين الأطراف وتشمل هذه الطريقة البنوك والمؤسسات الخاصة الأخرى التي يتم إنشاؤها لغرض الدفع الإلكتروني.

1- **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، المرجع السابق، ص327.

2- **جمال زكي الجريدلي**، البيع الالكتروني للسلع المقلدة عبر شبكة الانترنت، دراسة فقهية مقارنة، دار الفكر الجامعي، مصر، 2008، ص40.

ويمكن أن يكون من خلال شبكة عامة حيث يتم التعامل بين أشخاص لا تربطهم رابطة وهذه الشبكة يمكن أن تقاوم سواء كانت الجهة التي تقوم على إدارة الدفع الإلكتروني خاصة أو عامة[1].

الفرع الثاني

تعريف الدفع الإلكتروني

يقتضي منا الأمر التعريف بمصطلح الالكتروني أولا،لنطرق بعد ذلك إلى دراسة جوهر تقنية الدفع الالكتروني.

أولا- التعريف بمصطلح "الإلكتروني":

قدمت التشريعات الغربية تعريفات عديدة لمصطلح الكتروني، ففي قانون الولايات المتحدة الأمريكية الموحد يعرف بالمصطلح "الكتروني" بأنّه: «تقنية كهروبائية، رقمية مغناطيسية، بصرية، الكترومغناطسية أو أي شكل أخر من أشكال التكنولوجيا، يضم إمكانات مماثلة لتلك التقنيات». فهذا تعريف واسع يشمل كل وسيلة تعمل بالكهرباء أو المغناطيس أو غيرهما.

أما في القانون الفرنسي فان مصطلح الكتروني له أيضا معنى واسع بحيث يشمل كل قطاعات الاتصال عن بعد، حيث عرف جانب من الفقه التجارة الإلكترونية أنها "**استخدام لكل القطاعات الاتصال عن بعد**"[2].

ثانيا- تقنية الدفع الإلكتروني :

عرف التشريع الأمريكي أمر الدفع، وبالتحديد في التقنيين التجاري الموحد الأمريكي (Uniform commercial code) التحويل الصادر عن المصدر المصرفي بأنّه: «مجموعة الخطوات التي تبدأ بأمر التحويل الصادر عن المستفيد بهدف الدفع للمستفيد من

1-**Hubert de VAUPLANE**, le droit bancaire et la mondialisation des marchés financiers, R.J.C, le droit des affaires du xxi siècle, pp.190-191.

2- **جمال زكي الجريدلي**، البيع الالكتروني للسلع المقلدة عبر شبكة الانترنت، دراسة فقهية مقارنة، المرجع السابق، ص10.

الأمر، ويتم ذلك شفويا، الكترونيا أو كتابيا ويشمل ذلك أي أمر صادر عن بنك الآمر، أو البنك الوسيط يهدف إلى تنفيذ أمر الآمر بالتحويل، ويتم النقل بقبول بنك المستفيد دفع قيمة الحوالة لمصلحة المستفيد المبين في الأمر»[1].

كما عرفت العديد من التشريعات العربية التقنية نفسها بأنّها: «عقد بين الآمر بالتحويل المصرفي والبنك مصدر الحوالة يلتزم بموجب أن يدفع بنفسه، أو بواسطة غيره مبلغا من النقود يعادل قيمة الحوالة إلى المستفيد مقابل عمولة متفق عليها»[2].

إلى جانب ذلك صدرت العديد من التعاريف للدفع الإلكتروني مسايرةً لأوضاع ومتطلبات التجارة الإلكترونية فنجد القانون النموذجي للتحويلات الدولية للأموال (model law on international crédit transferts) الصادر في عام 1992 عن لجنة الأمم المتحـدة (unicitral) يعرف هذا القانون التحويل المصرفي بأنّه: «**مجموعة العمليات التي تبدأ بأمر الدفع الصادر عن الآمر بهدف وضع قيمة الحوالة تحت تصرف المستفيد**» ويشمل التعريف أي أمر الدفع صادر عن بنك الآمر أو أي بنك وسيط تهدف إلى تنفيذ أمر الدفع الصادر عن الآمر[3].

1-Article 4A-103, of the Uniforme Commercial Code (UCC) : «payment order means an instruction of a sender to a receiving bank, transmitted orally, electronically, or in writing to pay, or to cause another bank to pay a fixed or determinable amount of money to a beneficiary » by the American copyright, 2005, by the American law institute. In : www.law.cornell.edu

2- **محمد عمر ذوابة**، عقد التحويل المصرفي الالكتروني (دراسة قانونية مقارنة)، دار الثقافة للنشر والتوزيع، مصر، 2006، ص23.

3- المرجع نفسه، ص22. لتفاصيل أكثر أنظر: يعرف البعض تقنيات الدفع الإلكترونية بأنها"تقديم البنوك الخدمات المصرفية التقليدية أو المبتكرة ،من خلال شبكات اتصال إلكترونية، وتقتصر صلاحية الدخول إليها على المشاركين فيها وفقا لشروط العضوية التي تحددها البنوك ومن خلال أحد المنافذ على الشبكة كوسيلة لاتصال العملاء". أنظر: **محمود أحمد إبراهيم الشرقاوي**، مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي 10 و12 ماي 2003، ص17 منشور على الموقع http://slconf.uaeu.au

أنظر في ذلك، المادة 02 من القانون النموذجي للتحويلات الدولية للأموال الصادر عن لجنة الأمم المتحدة 1992، unicitral التي تنص:

«Credit transfer means the series of operations, beginning with the originator's payment order, made for the purpose of planning friend et the disposal of à beneficiary, the term includes any payment order issued by the origination bank or any intermediary bank intended carry out the originator's payment order… »

فيمكننا الاستناد إلى بعض التعاريف الدفع الالكتروني فعرفه الأستاذ "أيمن قديح" على أنّه: «**عملية تحويل الأموال في الأساس ثمن لسلعة أو خدمة بطريقة رقمية باستخدام أجهزة الكمبيوتر وإرسال البيانات عبر خط تليفوني أو شبكة ما أو أي طريقة لإرسال البيانات**»[1].

كما عرف المجلس الاقتصادي الفرنسي الدفع الإلكتروني أنّه: «**مجموعة التقنيات الإعلامية، المغناطيسية أو الإلكترونية...الخ. تسمح تحويل الأموال دون دعامة ورقية والتي ينتج عنها علاقة ثلاثية من بين البنك البائع والمستهلك».**

ثالثا- طبيعة الدفع الإلكتروني:

من خلال التعريف المقدم لمصطلح "**اليكتروني**" وجدنا انه يشمل كل وسيلة كهربائيـة أو مغناطيسية أو كهرومغناطيسية أو أي وسيلة أخرى لها إمكانات مماثلة تستخدم في تبادل المعلومات وتخزينها واسترجاعها، وطالما أنها وسيلة فلا تغير من حقيقة البيع في كل من الفقهين الإسلامي والقانوني[2]، وهي وسيلة تميز التجارة الإلكترونية عامة والدفع الإلكتروني خاصة، ولا مانع من استخدامها شرعا وقانونا[3].

1-الدفع الإلكتروني من حيث المبدأ :

من المعروف عامة أن الدفع هو تقديم مبلغ من المال مقابل اقتناء سلعة أو خدمة ومن الناحية القانونية هي وسيلة لانقضاء التزام المدين لدى الدائن، إذن الدفع يفترض وجود دين في ذمة المدين.

ولا يلتزم أن يكون الدافع هو المدين الأصلي، وإنّما دين يمكن أن يقوم به غير المدين الأصلي، أي من ينوب عنه[4].

1- **أيمن قديح**، الدفع الالكتروني من يحميه؟ مقال منشور على http://analyseer.net، 2006/06/09.

2 -**TOERING Jean Pierre et BRION François,** Les moyens de payements, Edition que sais-je? 1ère édition, Paris, 1999, p.32.

3- **جمال زكي الجريدلي**، البيع الالكتروني للسلع المقادة عبر شبكة الانترنت، دراسة فقهية مقارنة، المرجع السابق، ص56.

4 - **WERY Etienne**, Facture , Monnaie, Litec, Paris, 2003, p.43.

ويرى القانونيون أن الدفع الإلكتروني هو الاسم الطبيعي، المقدم لنوع من الدفع من بين الآخرين. ومن خصوصيات الدفع الإلكتروني هو استعمال وسيلة خاصة التي تكون بدورها ميكانيزم أو وسيلة تتم العملية كلها أو جزء منها على وسيلة الكترونية[1].

ونظرا للرهانات الكثيرة التي تثور بمناسبة هذه التقنية، نجد مثلا حماية مصالح المتعاملين (مختلف مستعملي هذه التقنية) عبر شبكة الإنترنت حيث أن مصلحة المشتري هو حماية دفعه للثمن عن طريق الشبكة.

وحماية البائع بتأمين استحقاقه لدينه، الشيء الذي يدفعنا إلى إلزامية توسيع النظر إلى طبيعة الدفع الإلكتروني فهو لا يعني بالضرورة أنه مرادف للدفع عبر الخط الإلكتروني ، لكنه يمثل تقنية مستعملة في شتى الميادين فنجد الملايين من مستعملي هذه الوسيلة أو الميكانيزم، لدفع واجبات المطعم، أو دفع حق المرور(Péage)، وكذلك استعمالها لسحب الأموال من الموزعين الإلكترونيين للأوراق[2]، كما يمس العديد من الشركات التي تقوم بتحويل الأموال والدفع بواسطة برنامج البنك على الخط...الخ[3].

أما عن طريقة الوفاء بالثمن فتحرص العقود في الغالب، على النص على أن يتم الوفاء على الخط أي الشبكة نفسها بواسطة بطاقة مصرفية أو محفظة النقود الكترونية[4].

1- **WERY Etienne**, Facture , Monnaie, Op.cit, p44.

2-Distributeur Automatique de Billet (DAB). In : une machine à une banque de branche ou d'un autre emplacement qui permet à un client d'effectuer de base bancaire, des activités contrôle de son équilibre, le retrait ou le transfert de fond même si la banque est fermée. In : www.investorwords.com./308/atm.html

3- Avec le développement de la banque en ligne de plus en plus de produit et services financier ou de produits d'assurance sont disponible sur internet : **Cathie-Rosalie Joly**, banque en ligne, guide de la dématérialisation de la souscription, article du 21/04/2008, in : www.droit-technologie.org

4- **عبد الرحمن بن عبد ا السند**، الأحكام الفقهية للتعاملات الالكترونية (الحاسب الآلي وشبكة المعلومات "الانترنت")، المرجع السابق، ص204.

2- الدفع الإلكتروني من حيث الأطراف:

يعتبر الدفع الإلكتروني أو الوفاء الإلكتروني تقنية معقدة لتحقيق أهدافها وتنفيذ التزامات مستعمليها، بما يستوجب تدخل أطراف أخرى لخصوصية هذه التقنية التي تتم عبر دعامات الكترونية، والتي يشترك فيها ثلاثة أشخاص أساسا:

أ- البنك أو المؤسسة المالية المقدمة لخدمة الدفع: وهي تلك التي تمنح العميل البطاقة بشروط محددة[1] والتي تقبل كذلك المعاملات الإلكترونية الأخرى كالشيك الإلكتروني، فالوسيط المالي في العقود الإلكترونية هو بنك أو مؤسسة مالية تقوم بنقل الثمن من المشتري إلى البائع في عقد البيع مثلا أو من المستخدم إلى المنتج في عقد المعلومات.

ويتم ذلك عن طريق التسويات المالية باستخدام نظام المعاملات الآمنة الذي يتم بواسطته نقل بيانات بطاقات الدفع ،حيث يؤكد هذا النظام شخصية حامل البطاقة أو عن طريق ما يسمى بالبنك المحمول وهو عبارة عن حاسوب شخصي متصل إلكترونيا بالبنك الأصلي الذي يقوم كوسيط مالي بالوفاء بالالتزامات النقدية لعملائه تجاه دائنيه[2].

ب-المشتري المرخص له باستعمال وسائل الدفع الإلكترونية: هو العميل الذي يحصل على البطاقة لاستخدامها فيما بعد في الوفاء بقيمة مشترياته أو للسحب من أجهزة الصراف الآلي.

ج-التاجر المرخص له التعامل بتقنيات الدفع الإلكترونية: هو الذي يقبل التعامل بالبطاقة مع العميل بناء على اتفاق مسبق بينه وبين المؤسسة مصدرة البطاقة.

1- **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية وسائل الدفع الالكترونية الحديثة، المرجع السابق، ص357.

2- **رضا متولي وهدان،** النظام القانوني للعقد الإلكتروني والمسؤولية عن الاعتداءات الإلكترونية، دار الفكر والقانون، الطبعة الأولى، المنصورة، 2008، ص27-28.

كما يرى البعض أن هناك وساطة أو تدخل متعامل اقتصادي في هذه العملية، وفي التجارة الإلكترونية عامة وهو الطرف الذي يستغل الوسائل الإلكترونية وبرامج الحواسب والتي يضعها تحد تصرف البنوك، والتجارة والمستهلكين[1] وفي شأن التجارة الإلكترونية يراد بمصطلح "الوسيط" فيما يتعلق برسالة بيانات معينة، الشخص الذي يقوم نيابة عن شخص أخر بإرسال أو استلام أو تخزين رسالة بيانات أو تقديم خدمات أخرى فيما يتعلق برسالة البيانات هذه[2].

كما عرف القانون النموذجي للأونسيترال شان التجارة الإلكترونية المراد بمصطلح "المرسل إليه" رسالة بيانات الشخص الذي قصد المنشئ أن يتسلم رسالة البيانات، ولكنه لا يشمل الشخص الذي يتصرف كوسيط فيما يتعلق بهذه الرسالة[3].

رابعا-خصائص الدفع الإلكتروني:

التجارة الإلكترونية بيئة غير مادية تتم فيها المعاملات التجارية لذا تغيب الدعائم الورقية فيها، ونظرا لدولية شبكة الإنترنت، فوسائل الدفع الإلكتروني المستعملة من خلالها تكون ذات طبيعة دولية أيضا، بمعنى أن تكون مقبولة من طرف جميع الدول، حيث أن عقد الاشتراك في بنوك المعلومات يتم عبر فضاء الكتروني مفتوح بين مستخدمين من مختلف الأقطار[4].

1- امتداد صفة دولية العقد الالكتروني إلى تقنية الدفع الالكتروني:

تضفي صفة الدولية على العقد الذي يتم عبر الإنترنت الذي يفترض تباعد أطرافه حيث يغيب الحضور المادي على مائدة المفاوضات أو ما يسمى بمجاس العقد، فوسيلة

1-**VOLLE Michel**, Economie des nouvelles Technologie, Internet, Edition Economica , Paris, 1999, p198.

2- **وائل أنور بندق،** موسوعة القانون الالكتروني وتكنولوجيا الاتصالات، دار المطبوعات الجامعية، الإسكندرية، 2007، ص19. أنظر في نفس السياق نص المادة الثانية من القانون النموذجي للاونسترال، بشأن التجارة الالكترونية، ديسمبر 1996.

3- المرجع نفسه، ص19.

4- **فاروق محمد أحمد الإباصيري،** عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة الجديدة للنشر، مصر، 2002، ص99.

الدفع الإلكتروني تستجيب لهذه السمة، حيث أنّها تكون وسيلة دفع لتسوية المعاملات التي تتم عن بعد، فيتم الدفع من خلال إعطاء أمر الدفع الذي يتم وفقا لمعطيات الكترونية تسمح بالاتصال المباشر بين أطراف العقد[1].

والنقود التي يتم من خلالها تسوية المعاملات عن طريق الدفع الإلكتروني يمكن أن تكون مخصصة سلفا لمباشرة هذا الغرض، حيث تتم عملية الخصم من المبلغ المخصص مسبقا لهذا الغرض.

إذن لا يمكن سحب معاملات أخرى عن المبلغ المخصص للدفع الإلكتروني بغير هذه الطريقة وهذا بالنسبة للعقود التي يكون فيها الثمن مصحوب بالدفع مقدما، وهذا ليس في كل الأحوال، حيث يمكن الدفع بالكروت البنكية العادية رغم عدم وجود مبالغ مخصصة لغرض الدفع سالفا [2].

2- من حيث الجهة التي تقوم بخدمة الدفع الإلكتروني:

يترتب على هذه الطبيعة تواجد نظام مصرفي مسبق لدى طرفي التعامل يتيح الدفع بهذه الوسيلة، أي توفر أجهزة تقوم بإدارة مثل هذه العمليات التي تتم عن بعد ومن شأنها أن توفر الثقة للمتعاملين بهذه الوسيلة، فيرتبط هذا الدور بصفة أصلية بالبنوك وغيرها من المنشآت التي تقوم لهذا الغرض، حيث أن إدارة وسائل الدفع في البلاد الأوروبية، عدا فرنسا، غير مقتصر على البنوك بغرض تسهيل تبادل وتقديم هذه الخدمة بين البلدان الأوروبية[3].

3- من حيث وسائل الأمان الفنية:

يتم الدفع الإلكتروني من خلال فضاء معلوماتي مفتوح، فإن خطر السطو على أرقام الكروت أثناء الدفع الإلكتروني قائم، فيزداد هذا الخطر في الدفع عبر الإنترنت عن

1- **فاروق محمد أحمد الإباصيري**، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، المرجع السابق، ص100.

2- المرجع نفسه، ص100.

3- نفسه، الصفحة نفسها.

غيرها من الشبكات باعتبارها فضاء يستقبل جميع الأشخاص من جميع البلدان بمختلف مقاصدهم ونواياهم.

لذلك يجب أن يكون مصحوبا بوسائل أمان فنية من شأنها أن تحدد هوية المدين الذي يقوم بالدفع والدائن الذي يستفيد منه، فتتم بطريقة مشفرة وبرامج خاصة معدة لهذا الغرض حيث لا يظهر الرقم البنكي على الشبكة الويب WEB، كما يتم عمل أرشيف للمبالغ التي يتم السحب عليها باستخدام هذه الطريقة يكون من السهل الرجوع إليه.[1]

خامسا- تقنية الدفع الإلكتروني في الجزائر:

لقد سعت الجزائر في خضم هذا التطور التكنولوجي الهائل الذي أصبح حتمية على كل دولة حتى تتأقلم وتصبح عنصرا فعالا في الاقتصاد والمبادلات الدولية إلى الاهتمام باستعمال هذه التقنية المصرفية.

وقد اهتمت الحكومة الجزائرية وعلى رأسها رئيس الجمهورية بقطاع البريد وتكنولوجيا الإعلام والاتصال، حيث أصبح خيار استراتيجي لتطوير هذا القطاع وترقية الاقتصاد الرقمي، الداخلي وتفاعله مع الاقتصاد العالمي، فإلى جانب الاستيراد الهائل للوسائل المادية قصد تحقيق هذه الأهداف تم وضع إستراتيجية منسجمة وكاملة لتحقيق ذلك.

فظهرت في أواخر التسعينات شركة "ساتيم" SATIM وهي شركة ذات أسهم تابعة للبنوك الجزائرية والتي ساهمت في وضع حلول في مجال التحويلات الإلكترونية ما بين البنوك الذي دخل حيز التنفيذ منذ عام1997. فعملت الشركة نفسها على وضع قناة وطنية للموزعين الأوتوماتكيين للأوراق المالية التي تنخرط فيه البنوك للاستفادة من هذه

1- من خلال هذه البرامج يتم وضع كود Code سري لتشغيل كارت البنكي، يجب الضغط أولا على كلمة السر Mot de passe الذي يتكون من كتابة عدة أرقام أو عبارات مركبة، يأخذ البرنامج عدة لحظات ويتم خلق الكود السري الذي يتكون من رقم الكارت البنكي، نوعها، صاحبها، العنوان، رقم الهاتف. أنظر في ذلك: **فاروق محمد أحمد الإباصيري**، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، المرجع السابق، ص102.



الخدمات وقد عملت هذه التقنية على القيام بحوالي مليون عملية سنويا عن طريق 300 موزع الأوراق المالية[1].

كما نص قانون النقد والقرض 2003-11 في المادة 69 منه على الاعتراف باستعمال كافة وسائل الدفع التي تسمح للأشخاص تحويل الأموال مهما كانت الدعامة أو الطريقة المستعملة[2] ومن خلالها يمكننا أن نستنتج أن المشرع نص على إمكانية استعمال كافة تقنيات ووسائل الدفع التقليدية والإلكترونية.وحسب تقديرنا فهو اعتراف ضمني لاستعمال هذه الوسائل،فهذا مؤشر إيجابي وقفزة معتبرة نحو تنظيم استعمال هذه التقنية عبر قنوات مفتوحة كالانترنت.

وتمت عدة محاولات لغرض توفير خدمات الدفع بالبطاقات البنكية من طرف بنكين هما BADR وCPA، هذه الأخيرة التي كانت السباقة في استعمال البطاقة البنكية لتطوير خدماتها[3] وحسب مدير (de la monétique)، فتجربة الجزائر في هذا المجال كانت منذ 1994، حيث تم إحداث من طرف بنك الفلاحة والتنمية الريفية (BADR) بطاقة الدفع، ولم يكن البنك يحتوي إلاّ على موزعين رقمين على مستوى العاصمة ثم ساهمت العديد من المؤسسات البنكية الوطنية منها والأجنبية بوضع شبكة للدفع الالكتروني ووصل عدد الموزعين الآليين للنقود سنة 2008 إلى 919 موزع الكتروني على المستوى الوطني[4].

1-**BEN KADI Aissa**, **BELLADJEL Nassima, OUGHANEM Ali,** la monétique (une fonction d'avenir), mémoire de licence en sciences économique option : monnaie, finance, banque, université Mouloud Mammeri, Tizi-Ouzou, 2003, pp.87-88.

2-«Sont considérés comme moyens de paiement tous les instruments permettant à toute personne de transférer des fonds et ce, quel que soit le support ou le procédé technique utilisé», article 69 de l'ordonnance 2003-11 du 27 joumada ethania correspondant au 26 aout 2003 relative à la monnaie et le crédit. Jora no 52 du 27/08/2003.

3- le CPA à mis en place un ensemble de cartes bancaires tel que le carte CPA-CASH et la carte CPA-VISA ainsi que l'affiliation au réseau international en acceptant le paiement par MASTER –CARD et EUROCHEQUE. Voir : **BEN KADI Aissa**, **BELLADJEL Nassima, OUGHANEM Ali,** la monétique (une fonction d'avenir), op.cit, p.106.

4-**BENCHOHRA Kara**, le commerce électronique en Algérie défis et perspectives, mémoire de fin d'étude pour l'obtention du diplôme d'ingénieur d'état en planification et statistiques, institut national de la planification et de la statistique, Alger, 2008, p76.

وقد عددت الجزائر حوالي ثلاثة ملايين من بين الأشخاص المستعملين للانترنت سنة 2006 حسب قرار رسمي نشرته الوكالة الجزائرية للصحافة، كما تم إحصاء حوالي 700.000 رخصة استعمال النظام ADSL في سنة 2006 التي لم تكن موجودة أصلا سنة 2000 وفي السنوات الأخيرة بادر البنك الجزائري بوضع مشروع لتطوير القطاع البنكي بمساعدة البنك العالمي(1).

وظهرت عدة محاولات كذلك لخلق نظام الدفع الإلكتروني من طرف شركة الخطوط الجوية الجزائرية، كما حاول أحد الخواص صاحب العنوان (Maktibn.com) تطوير التجارة الإلكترونية في الجزائر بحيث أعد مشاريع حول بطاقات الدفع مع شريكتي (CSC et Gepcom)، وحسب تصريحات نفس المسؤول فان كافة الشروط متوفرة لإعطاء إشارة الانطلاق للتجارة الإلكترونية، خاصة وأنّه يوجد حاليا أكثر من 100 عنوان للتجارة الإلكترونية في الجزائر.

رغم ذلك تبقى الجزائر بعيدة كثيرا مقارنة بجيرانها المغرب، تونس في مجال الصيرفة الالكترونية(La Monétisation)، وحسب إحصائيات قامت بها الجزائرية للاتصالات، على الجزائر مضاعفة 15 مرة من حجم استعمال للدفع الإلكتروني للالتحاق بمستوى تونس والمغرب ومضاعفة بـ 750 مرة للالتحاق بمستوى الدول الأوروبية.

سادسا- رهانات وتحديات الدفع الإلكتروني:

تعتبر عملية الدفع الإلكتروني التي تتم برسائل بيانات عبر الإنترنت من أهم ممارسات التجارة الإلكترونية المستحدثة وذلك يترجم بضخامة العمليات التحويلية للأموال التي تتم بالطريقة نفسها، والتي تحمل في طياتها رهانات وتحديات كبيرة في ظل ثورة التكنولوجيا.

1-**BOUAISSA Karim**, Le commerce et la vague Internet, Mémoire de licence en Management faculté des sciences de gestion, Laghouat, Algérie, publié sur site : www.memoireonline.com

1- رهانات الدفع الإلكتروني:

تجد تقنيات الدفع الإلكتروني مجالها الخصب في رحاب التجارة الإلكترونية التي يعمل مؤطروها على تطويرها نظرا لأهميتها واستعمالها من طرف ملايين المستهلكين ومختلف المتعاملين عبر العالم الشيء الذي دفع بمجموعة من البنوك إلى استحداث اتحادات قصد التحكم الجيد في هذه العملية وتنظيمها تنظيما محكما كإتحاد (Americana Express et Dîners).

فبعد ظهور هذه التقنية في الولايات المتحدة الأمريكية في أواخر الأربعينات من القرن الماضي واستعمالها من طرف الشركات البترولية والمؤسسات التجارية لبطاقات دفع خاصة بها، انتشرت هذه الوسائل بصفة مذهلة في أوربا خاصة وهذا ما خلق منافسة بين المؤسسات بتقديم أفضل العروض بأدنى العمولات.

فعلى سبيل المثال دفعت هذه الثورة المعلوماتية البنوك الفرنسية من بينها (Société Générale, Crédit Lyonnais, BNP) إلى استحداث وسيلة جديدة بهدف إحداث وسيلة الكترونية للدفع البنكي ذات المبالغ الضخمة ثم طور هذا النظام إلى إمكانية السحب في 1970، وفي 1971 تم إنشاء تجمع ذات المصالح الاقتصادية "البطاقة الزرقاء" [1]، وتم في 1984 إنشاء البطاقات البنكية بهدف تقريب كل مصدري البطاقات الفرنسيين لتخفيض ثمن العملية وتحسين الخدمات ومن بين أهداف هذه الاتحادات :

- التنسيق التقني بين المؤسسات المالية لإصدار بطاقات الدفع.
- إيجاد شبكة مشتركة لقبولها.
- التنظيم القانوني المحكم لهذه العملية المصرفية[2].

1-**TOERING Jean Pierre et BRION François,** les moyens de payements, op.cit, p.33.

2 - كما تم في 1977 ربط نظام البطاقة الزرقاء بالشبكة العالمية لتأمين خدمات موحدة. أنظر: Ibid, p.33

2- تحديات الدفع الإلكتروني:

يمكننا اعتبار مواجهة المخاطر والتهديدات التي يتعرض لها الدفع الإلكتروني من بين تحديات هذه التقنية، فمن جهة تعتبر هذه المخاطر مشتركة بين جميع حالات استعمال وسائل الدفع التي يضاف إليها من جهة أخرى المخاطر الناتجة عن الاستعمال المفرط للتكنولوجيا وهذا ما أشار إليه تقرير "**مان**" رقم 28 الذي يستخلص أربعة (04) نقاط ضعف تعتري هذه التقنية والمبينة علميا نذكرها كالأتي:

- نظرا لفقدان التحكم في الوسيلة الرقمية من طرف المرسلين، والذين لا يكونون بإمكانهم ضمان اشتراك أنظمة المعلوماتية بوسائل الدفع بإمكانها تأمين مستوى الخدمات المضمونة للمستعملين[1].
- خطر مالي في حالة سوء استعمال إرادي أولا بوسيلة دفع، والذي يؤدي إلى خسارة مالية لمجمل المتعاملين المشتركين في العملية.
- خطر تبييض الأموال، مدعم من الطبيعة غير المادية للعلاقة بين الأطراف العملية الإلكترونية والتي يصعب مراقبة هويتهم ومراقبة عملياتهم المالية غير المستقرة.
- مشكلة فقدان الثقة في النقود في حالة إساءة في استعمال وسائل الدفع الإلكتروني[2].

خاصة وحسب تقرير منظمة العالمية للتجارة الذي تم نشره عام 2004 فإن نسبة المعاملات المتوقع إجراؤها عبر شبكة الإنترنت عام 2010 تبلغ نحو 70 بالمائة من حجم التجارة الدولية كلية[3].

---

1 - **WERY Etienne**, Facture , Monnaie op.cit, p 46.

2 - Ibid, p 47.

3- **أيمن قديح**، الدفع الالكتروني من يحميه؟ مقال منشور على http://analyseer.net، 2006/06/09، ص2.

المطلب الثاني

البيانات الإلكترونية واقع المعاملات المالية الحديثة

دفع انتشار النظام الرقمي، والمعالجة الإلكترونية للبيانات إلى الزوال التدريجي للطبيعة المادية للعلاقات القانونية، وهذا بعدما كانت الدعامات الورقية هي الوسيلة المستعملة في كافة العلاقات والمراسلات بين المتعاملين الاقتصاديين منذ إرسال خطابات النوايا للتعاقد مرورا بمرحلة التفاوض بمبادلة الوثائق لكي تكون حجية على الأطـراف في التعاقد بتحرير البنود المتفق عليها على صفحات ورقية.

فأصبحت المعاملات في يومنا هذا ومنذ فترة زمنية معتبرة تعتمد على دعامات الكترونية أو ما يسمى (La dématérialisation) أي تنحية الطابع المادي للدعائم وذلك بالمعالجة الرقمية للبيانات. واعتبر الفريق العامل المعني بالتجارة الالكترونية التابع للأمم المتحدة أن الأشكال الالكترونية للاتصالات التي يغطيها قانون الاونسيترال النموذجي للتجارة الالكترونية ينبغي أن تعتبر أيضا كتابة[1].

وذلك ردا على فريق من الكتاب الذي قال أن الرسائل المرسلة عن طريق الحاسوب لا تفي بشروط الكتابة، وذلك على أساس أنه ليس هناك نسخة مادية يجري تسلمها.

الشيء الذي يدفعنا في نطاق بحثنا إلى التساؤل عن حجية هذه البيانات التي تخلو من الطبيعة المادية الملموسة والتي تتداول عبر شبكة الاتصالات العالمية، ففرضت ضرورة تأطيرها القانوني لتبيان حجتها، فيسجل واقع الاستخدام الحالي لشبكة الإنترنت تقدما ملحوظا لصالح تبادل الصفقات على حساب تبادل المعلومات بعد أن عدت التجارة في هذه الشبكة حقيقية وواقعا، فعدد الشركات العارضة تتزايد يوما بعد يوم ولاسيما من خلال مواقع الشبكة العنكبوتية (فرع الأول).

1- وثيقة لجنة الأمم المتحدة للقانون التجاري الدولي، الفريق العامل المعني بالتجارة الالكترونية، الجوانب القانونية من التجارة الالكترونية، الدورة 38 نيويورك من 12-23 مارس 2001، ص10.

هذه التقنية التي أحدثت ثورة حتى في النقود التي تعتبر الوسيلة أو العمود الفقري للمعاملات التجارية فكان من المنطقي أن تحمل التجارة الإلكتروني وسيلة لاستيفاء الدفع وهذا ما تم استحداثه في إطار ما يسمى بالنقود الإلكترونية ، حيث اختلفت الاتجاهات التي تعترف بحجتها القانونية من عدمها ، وإحداث ما يسمى بالبنوك الإلكترونية إلى جانب النقود الرقمية [1] (فرع الثاني).

ونظرا لعدم الوجود الفعلي لمجلس العقد في التعاقد عن بعد، حيث يتم إرسال البيانات من طرف إلى أخر، يستوجب انساب هذه الالتزامات إلى صاحبها الحقيقي الذي يعبر عن إمكانيته لتحمل الالتزامات مما يستدعي إلى انساب التوقيعات الإلكترونية إلى أصحاب العلاقة القانونية (فرع الثالث).

الفرع الأول

ماهية البيانات الإلكترونية

إن العلاقة الثلاثية التي تنشأ عن الدفع الإلكتروني تتم بإرسال بيانات سواء ما تعلق بالمعلومات الخاصة بالمشتري بإرسال شيك الكتروني أو بإرسال رقم بطاقة الدفع، أو ما تعلق بإرسال أمر الدفع، أو بالتحويل المالي ما بين البنوك (L’interbancaire).

وكتب الفقيه الفرنسي "ميلور" Mellor في عام 1972: **«إن للكمبيوتر شراهة لجميع المعلومات على نحو لا يمكن وضع حد لها وما يتصف به من دقة ومن عدم نسيان ما يخزن فيه، قد يقلب حياتنا رأسا على عقب يخضع فيها الأفراد لنظام رقابة صارم ويتحول المجتمع بذلك إلى عالم شفاف تصبح فيه بيوتنا ومعاملاتنا المالية وحياتنا العقلية والجسمانية عارية من الشاهد»**.

1- **عبد الرحمن بن عبد ا السند**، الأحكام الفقهية للتعاملات الالكترونية (الحاسب الآلي وشبكة المعلومات "الانترنت"، المرجع سابق، ص36.

أولا- تعريف الرسائل الإلكترونية :

تعرف الرسائل الإلكترونية بأنّها «**مجموعة الاتصالات الإلكترونية بين طرفين بهدف حصول على المعلوماتية**»[1]، فتبادل البيانات الكترونيا هو مجموعة المعايير المستخدمة في تبادل بيانات المعاملات الإلكترونية بين أجهزة الكمبيوتر التابعة للشركاء التجاريين وتنفيذ الصفقات التجارية بطريقة الكترونية بدون استخدام دعامة ورقية، وتسمى كذلك تعبيرا عن الرسالة الإلكترونية (Elecronic Mail)، وهي شعاع نظام انتقال المعلومات [2].

1- تعريف البيانات:

البيانات عبارة عن حقائق وأفكار وأراء تصف حدثا معينا دون إجراء أي تعديل أو تفسير أو مقارنة، حيث يتم الوصف لها بكلمات وأرقام أو رموز، ولذلك تعتبر البيانات هي المواد الخام التي تشتق منها المعلومات(Information).

والمعلومات تعرف بدورها بيانات لكن تمت معالجتها لكي يستفاد منها في عملية معينة بين المتعاملين، فهي بيانات خضعت للتحليل والتفسير[3].

وعرف المشرع الأمريكي المقصود بالمعلومات في قانون المعاملات التجارية الإلكترونية الصادر في سنة 1999 في المادة 10/2 منه بأنّها: «**تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر، البرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك**»[4] ويمكننا القول أن المشرع الأمريكي قد أعطى

1- **محمد دباس الحميد، ماركو إبراهيم نينو،** حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، ط1، عمان- الأردن، 2007، ص11.

2 - **TORTELLO Nicole**, **LOINTIER Pascal**, Internet pour les juristes, op.cit., p 69.

3 - **محمد دباس الحميد، ماركو إبراهيم نينو،** حماية أنظمة المعلومات، المرجع السابق، ص17.

4 - **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص94.

انظر في ذلك:

Section 2/ 10 Uniforme electronic transaction etc. Information: Means Data, image, sound, codes, computer programs , soft ware, databases.

مفهوما واسعا للبيانات بحيث ترك المجال مفتوحا لوسائل نقلها عند استعمال في أخر المادة عبارة "أو ما شابه ذلك".

2- قنوات نقل البيانات:

يتم نقل وتبادل البيانات والمعلومات الكترونيا عبر مواقع الويب باستخدام برامج التصفح مثل برنامج (Internet explorer) وبرنامج (Netscape communication) وتحويل البيانات والملفات، باستخدام بروتوكول نقل الملفات(FTP)[1].

وهي معايير متفق عليها دوليا لتبادل المعلومات بين الشركاء التجاريين، يسمى معيار تبادل بيانات الإدارة والتجارة، والنقل الكترونيا في الأمم المتحدة (UN/EDIFACT)[2].

هذا ما سعت إليه اللجنة الفرنسية للتنظيم والتأطير البنكي في قرارها المؤرخ في 20 أكتوبر 1992، الذي يرغم الانتقال الإلكتروني بين البنوك للأعمال التجارية بداية تاريخ 03 ماي 1994 [3].

كما اعتمد قانون اليونسترال النموذجي لشأن التجارة الإلكترونية الصادر في 1996 تعريفا للرسالة بيانات في الفقرة (أ) من المادة الأولى حيث نصت: «**يراد بمصطلح رسالة البيانات" المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة ، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات أو البريد الإلكتروني أو البرق، أو التلكس، أو النسخ البرق**»[4].

---

1 - **خالد ممدوح إبراهيم،** إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص59.

2- وفي هذا الإطار طورت عدد من المنشآت التجارية في مختلف قطاعات الأعمال. معيار متفق عليه دوليا لتبادل المعلومات بين الشركاء التجاريين، يسمى هذا المعيار، نظام تبادل البيانات الإدارة والتجارة والنقل الكترونيا في الولايات المتحدة الأمريكية UN/EDIFACT وكذلك معيار ANSI- X- 12 .أنظر: **خالد ممدوح إبراهيم،** المرجع نفسه، ص93.

3-**JEANTIN Michel**, Droit Commercial, Instrument de Paiement et de Crédit, entreprise en difficulté, Dalloz Delta, 4 eme Edition, Paris, 1995, p263.

4- **وائل أنور بندق،** موسوعة القانون الالكتروني وتكنولوجيا الاتصالات، المرجع السابق، ص19.

أنظر في ذلك: نص المادة الأولى من القانون اليونسترال النموذجي بشأن التجارة الالكترونية.

فأدى ظهور التبادل الإلكتروني للبيانات في إطار التكنولوجيا الجديدة للاتصال والإعلام (NTCI) إلى ضرورة وضع تشريع محكم لمجال التجارة الإلكترونية، نظرا لما تمتاز به هذه التجارة من تجريدها من الصفة المادية باستثناء عقد التبادل البياني أو ما يسمى (Echange de données informatisées) الذي يعقده أطراف العلاقة خاصة ما بين البنوك، فهذا العقد لا يمكن تجريده من الصفة المادية، وإنما يخضع لظروف التعاقد والتعامل الكلاسيكية والاعتماد على الدعائم الورقية [1].

وفي المادة 2/2 من قانون الأونسيترال النموذجي للتجارة الإلكترونية عرفت تبادل البيانات الإلكترونية بأنّه «**نقل المعلومات الكترونيا من كمبيوتر إلى كمبيوتر باستخدام معيار متفق عليه لتكوين المعلومات**»[2].

ويرى بعض القانونيين أن نقل المعلومات من كمبيوتر إلى كمبيوتر عبارة حصرية إلى حد ما، فيمكن أن تنتج المعلومات على الكمبيوتر ويتم تخزينها في شكل رقمـ ـي (في قرص مضغوط مثلا) ونقلها يدويا لتسترجع فيما بعد في الكمبيوتر الأخر[3].

كما عرف جانب من الفقه الأمريكي بأنها: عملية تبادل البيانات (Transaction) وإبرام العقود بين أطراف محددة بطريقة الكترونية ومن خلال الكمبيوتر[4].

3- جهود بنك الفلاحة والتنمية الريفية BADR كنموذج في المعاملة بالبيانات:

لقد قام بنك الفلاحة والتنمية الريفية تماشيا مع مستجدات الوضع الراهن الذي فرضته التجارة الإلكترونية باقتناء وسائل حديثة وتسخير مراكز جديدة لتوفير المعاملة بوسائل الدفع الحديثة، وذلك اعتمادا على التجربة التي اكتسبتها من نظام (SYRAT) الذي

---

1 - **TORTELLO Nicole**, **LOINTIER Pascal**, Internet pour les juristes, op.cit., p.154.

2 - راجع: المادة 2/2 من قانون اليونسترال النموذجي للتجارة الالكترونية، الصادر في 16 ديسمبر 1996 عن هيئة الأمم المتحدة.

3 - **ممدوح محمد خيري هاشم**، مشكلات البيع الالكتروني عن طريق الانترنت في القانون المدني، دراسة مقارنة دار النهضة العربية، دون طبعة، مصر، 2000، ص66.

4 - **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص95.

وضع في عام 1996 والذي يوفر نوعا من الضمان والخبرة للمعاملة بالوسائل الإلكترونية.

فيعتبر بنك الفلاحة والتنمية الريفية السباق إلى المعاملة بالشيك الإلكتروني في الجزائر (La dématérialisation des chèques)، واتخذ هذا المشروع مراحل عديدة منها مرحلة اقتناء المعدات اللازمة للوكالات المتواجدة عبر التراب الوطني وكذا مرحلة تكوين المستخدمين لرفع مستوى التأهيل للتعامل بهذه الطرق.

ويتمثل هذا النظام الجديد في معالجة الشيكات إلكترونيا باستعمال جهاز سكانير (Scanner) ويسمح لمستعمليه من تخليص الشيكات في آجال قصيرة ومن بين محاسنه كذلك تقليص تكاليف تخليص الشيكات فأصبحت 117 دج بعدما كانت 234 دج.

وتجدر الإشارة إلى أن هذا النظام لا يمس سوى الشيكات على الوضع الحالي إلاّ أنه وبصفة تدريجية سيمس استعمال بطاقات الدفع، والتحويلات الإلكترونية ... ومن أجل تحقيق ذلك عادة ما ينظم البنك أيام دراسية وملتقيات قصد تطوير تقنية المعلوماتية في المعاملات البنكية، وقد تم تزويد مختلف وكالات البنك بمراكز رقمية (Station numérisée) لتسهيل استغلال النظام.

كما تم اقتناء أجهزة سكانير وآلات طباعة وحواسيب محمولة لتحقيق فعالية النظام وتسخير خبراء في المعلوماتية قصد التدخل في كل الأحوال في كل ما يتعلق بالنظام[1].

4- التعاون الدولي في مجال التبادل الإلكتروني للبيانات:

تؤدي ضرورة إنجاح استغلال تكنولوجيا الاتصال والإعلام الجديدة لخدمة المتعاملين الاقتصاديين وتحقيقا لأهدافهم إلى ضرورة التعاون الدولي بتوحيد المقاربات في شتى مجالات التجارة خاصة فيما يتعلق بالتبادل الإلكتروني للبيانات.

فكانت أول محاولة دولية لإحداث التناسق في الممارسات المتعلقة بالسلوك الموحد للتبادل الإلكتروني للبيانات التجارية بواسطة الإرسال بعد سنة 1987 تحت رعاية غرفة

1- SYRAT est un nouveau système de traitement qui a été conçu et élaboré par les imageries informatiques de la BADR. B.I, Modernisation des moyens de paiement, un système entièrement automatisé, Revue BADR Info, N° 42, mai/juin, 2006, p.12.

التجارة الدولية، بهدف إيجاد نموذج لاتفاقات أو ما يسمى باتفاقية إطار لأنظمة تبادل البيانات، تختار الأطراف المعنية من نصوصها ما تراه أوفى بتحقيق أهداف علاقاتهم. وذلك بوضع قواعد السلوك الموحدة لتبادل البيانات باستخدام الإرسال الإلكتروني [1].

كما تعددت جهود المؤسسات الدولية من أجل وضع القواعد المنسقة للتبادل السالف ذكره من أجل نمو التجارة الإلكترونية، مـن بينها اللجنة الاقتصادية لأوروبا (Economic Commission For Europ) التي وضعت قواعد متعلقة بنقل البيانات الإلكترونية في مجال الإدارة والتجارة وتعرف باسم (UN/EDIFACT)[2] قصد إعطاء دفع أقوى لاستعمال الإنترنت ومحاولة تنظيم المعاملات والعلاقات القانونية التي تنشأ بين المتعاملين بها.

وسعت في نفس السياق لجنة المجموعة الأوروبية في توصيتها الصادرة في 18 ديسمبر 1987 التي دعت في حيثياتها إلى ضرورة التطوير السريع لخدمات البنوك والتجارة والصناعة في مجال الاتصالات والإعلام، للاستفادة من الدعائم التكنولوجية التي ترقي وسائل الدفع الإلكتروني[3].

فسارت التشريعات الداخلية في السياسة نفسها باعتماد هذه التقنية داخليا من طرف العديد من المؤسسات ونذكر على سبيل المثال: ففي تونس مثلا تم الاتفاق بين العديد من الشركاء البنكيين مثل جمعية المحترفين البنكيين (APB) والبنك المركزي التونسي والعديد من الشركاء إلى اعتماد اتفاق تعاون من أجل استعمال وتطوير الدفع الإلكتروني بالبطاقات (T.P.E)، كما انخرطت العديد من البنوك إلى هذا النظام تماشيا مع مستجدات التكنولوجيا للاتصال والإعلام، وكذا تأمين هذه المعاملات المصرفية بينها باعتماد نظام الدفع المؤمن (SPS)[4].

1- كما سعت الكثير من المنظمات الدولية منها المنظمة البحرية الدولية ومنظمة الأمم المتحدة للتجارة والتنمية التي ابتكرت عدة أنظمة التي تقوم على أساس التبادل الالكتروني للبيانات راجع: **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص96.

2 - **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص96.

3-Recommandation de la commission du 8 Décembre 1987 portant sur un code européen de bonne conduite en matière, 2005, www.balnet.net, p.1.

4- STEG: Lancement du paiement électronique des factures, in : http://www.dahnet.2005, p.10.

الفرع الثاني

النقود الرقمية المجردة من الطابع المادي

أولا- النقود الرقمية واقع قانوني أم وهم اقتصادي؟

لقد أثارت النقود الرقمية التي أوجدتها متطلبات التجارة الإلكترونية جدلا حول تكييفها وطبيعتها، فيرى البعض أن هذه الوسيلة ما هي إلاّ وسيلة أو نوع من النقود الكلاسيكية التي تجرد من طبيعتها المادية والتي تعبر عن انتقالها [1].

فيرى البروفسور "فاسور" Vasseur أن العلامة النقدية الفعلية تكمن في إمكانية استعمالها مباشرة عن طريق الوسيلة التي يتم بواسطتها الدفع، وإمكانية استعمالها المباشر من طرف متلقيها بدوره، فبوجود وسيط لا يمكن التحدث عن نقود، وفي هذا الصدد إذا أسقطنا هذه الفكرة على محفظة النقود الإلكترونية، هل تسمح لنا بنقل مبلغ معين من وإليها دون وسيط؟ وهل يمكن استعمال هذه النقود مباشرة دون المرور بالوسيط البنكي؟[2] يمكن للنقود الإلكترونية أن تلعب الدور الاقتصادي الذي تلعبه النقود التقليدية إذا كان الحامل هو الوحيد الذي يعرف قيمة الدين الذي يدفعه، وفي وقتنا الحالي لا يوجد وسيلة تستأثر على مجموعة الشروط التالية للقول بفعلية النقود الإلكترونية كنقود مستقلة عن النقود التقليدية ذات الطابع المادي الملموس، وتتمثل في شرط كونها:

---

1 - **SCHWERER François**, De la circulation électronique de monnaie scripturales à la monnaie électronique universelle, Revue Juridique Commerciale, 2001, p.56.

وقد أثار جدل فقهي حول طبيعة النقود الالكترونية فهل هي أموال تؤدي نفس الوظائف التي تؤديها الأموال وهل تعتبر نوع جديد من الأموال يضاف إلى الأموال النقدية والمكتوبة أم أنها تنتمي إلى وحدات من هذه الأنواع فالإجابة على هذه التساؤلات ستحدد النظام القانوني الذي ينطبق على النقود الإلكترونية. فإذا كانت تنتمي إلى نوع معين من هذين النوعين انطبق النظام القانوني لهذين النوعين، أما إذا كانت هذه النقود تمثل نوعا جديدا من الأموال، فيجب أن يحكمها نظام قانوني يتماشى وطبيعتها الخاصة أنظر في ذلك: **شريف محمد غنام،** محفظة النقود الإلكترونية، رؤية مستقبلية، بحث مقدم في مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانـون، دبي، 10 و12 ماي 2003 ص 118. منشور على الموقع الالكتروني: http://slconf.uaeu.acae

2-Elle ne peut apparaître vraiment que si le porteur est le seul à connaître le montant de sa créance sur l'émetteur. Voir: **SCHWERER François**, op.cit., pp.57-58.

- نقود الكترونية مسجلة في حساب كامل في دفاتر المؤسسة مصدرة النقود الالكترونية (L’émetteur).
- إمكانية القيام بالدفع أو تحويل دون إخطار في المؤسسة المالية مصدرة النقود الالكترونية (L’émetteur).
- إمكانية القيام بالدفع أو تحويلات بين الحاملين وبين الحاملين والتجار، دون المرور بالحساب البنكي التقليدي.

ولقد تعددت التسميات المقدمة لها فيسميها البعض النقود الرقمية، والبعض الأخر النقود الإلكترونية، وهي مقابل لقيمة السلعة أو الخدمة التي يدفع عبر شبكات الاتصـالات وتعتبر كنتيجة منطقية للتجارة الإلكترونية التي جردت المعاملات التجارية من مظهرها المادي وهذا ما يسمى (La dématérialisation) وصلت هذه النتيجة إلى تجريد النقود المألوفة الورقية أو القطع من صفتها المادية وأصبحت على شكل معلومات أو رموز ينقضي بها التزام الدفع.

من هنا كان لا بد من البحث عن وسيلة تتفق مع طبيعة التجارة الإلكترونية التي تتم عبر الإنترنت.

نظرا لأهمية ضبط المفاهيم الجديدة في مجال التجارة الإلكترونية، اهتم الكثير بتعريف النقود الإلكترونية لتحديدها وحصرها في وسائل محددة لترقية التجارة الإلكترونية.فتتمثل النقود الإلكترونية في وحدات إلكترونية رقمية يتم انتقالها بطريقة معينة من حساب شخص إلى حساب شخص أخر.

تخزن هذه الوحدات إما في ذاكرة كمبيوتر صغير ملتصق في كارت يحملها المستهلك (Chip Card) بحيث يستخدمها في الوفاء عن طريق هذا الكارت، أو تخزن في ذاكرة الكمبيوتر (Computer Memory) الشخصي للمستهلك بحيث يستخدمها عن طريق هذا الكمبيوتر لسداد أثمان البضائع والخدمات مثلها مثل النقود التقليدية فهي لا تحتوي

على نقود ورقية أو حقيقية وإنّما على وحدات يتم انتقالها بشكل إلكتروني وتمثل قيم مالية محددة[1] وظهرت عدة مقاربات للتعريف النقود الالكترونية:

أ- المقاربة على المستوى الأوروبي: إن ترقية التجارة الإلكترونية أصبحت هدفا سياسيا في أوروبا، وكنتيجة لذلك في 18 سبتمبر 2000، اعتمد الاتحاد الأوروبي التوصية 46/ 2000 التي تنظم المؤسسات التي توفر النقود الإلكترونية، وكذا استعمالها ومراقبة هذه المؤسسات.

وفي نفس التوصية تم تعريف النقود الإلكترونية كما يلي: «**قيمة نقدية تمثل دين على من يصدرها والتي يتم تخزينها على دعامة الكترونية، ومصدرة مقابل دفع مبلغ قيمته لا يمكن أن يقل عن قيمة النقدية الإلكترونية المصدرة، والتي تقبل كوسيلة دفع من قبل المؤسسات غير المؤسسة المصدرة لها**»[2].

وفي تقرير له عرف البنك المركزي الأوروبي سنة 1998 بما يمكن تسميته بالنقود الإلكترونية أنّها «**قيمة نقدية مخزونة الكترونيا على دعامة الكترونية كبطاقة أو ذاكرة حاسوب والمقبولة كوسيلة دفع من قبل المؤسسات الأخرى غير المؤسسة المصدرة لها**»[3].

كما عرفها المجلس الاقتصادي والاجتماعي الأوروبي أنّها «**مجموعة تقنيات رقمية، مغناطيسية، الكترونية، تسمح بانتقال النقود وتبادلها بدون دعامة ورقية**»[4].

1- **شريف محمد غنام،** محفظة النقود الإلكترونية، رؤية مستقبلية، المرجع السابق، ص104.

2-**WERY Etienne**, Facture, Monnaie et paiement, électronique, aspects Juridique, Op.cit, p.111, Voir aussi : Directive du Parlement Européen et cours UE, dir N° 2000 46/ CE, 18 Septembre, 2000, concernant l'accès à l'activité des établissements.

3- **SOUSI Blanche**, Actualités européennes, Revue de droit des affaires internationales, N° 2, 1999, p.238.

4- le paiement électronique est « *L'ensemble des techniques informatique, magnétiques, électroniques et télématiques permettant l'échange de fonds sans support papier* ». **TOERING Jean Pierre et BRION François,** les moyens de payements, Edition que sais-je? op.cit, p. 32

ب- المقاربة على المستوى العربي: ظهرت عدة محاولات لتعريف النقود الرقمية من طرف الفقه العربي، فعرفها البعض أنّها «**دفع أو تحويل الودائع المعالجة إلكترونيا ضمن أنظمة البنوك الإلكترونية**» غير أن الملاحظ من هذا التعريف يتطرق إلى تحويل القيمة إلكترونيا، دون أن يتطرق إلى تعريف القيمة النقدية نفسها.

فيما ذهب رأي آخر إلى أن النقود الإلكترونية هي «بطاقات تحتوي على مخزون إلكتروني أو أرصدة نقدية محملة إلكترونيا، على بطاقة تخزين القيمة» ويعاب على هذا التعريف أنّه لم يعرف النقود الإلكترونية بل عرف الوسيلة التي يتم فيها خزن أو حفظ تلك النقود.

وقدم فريق أخر تعريف أكثر دقة فالنقود الإلكترونية عبارة عن «**سلسلة من الأرقام التي تعبر عن قيمة معينة ، تصدرها البنوك التقليدية أو الافتراضية لمودعيها ويتحصل هؤلاء عليها في صورة نبضات كهرومغناطيسية، على كارت ذكي أو القرص الصلب**» ويعرفها الأستاذ "هيثم عدنان عزو" أنّها «**عبارة عن قيمة نقدية بعملة محددة تصدر في صورة بيانات إلكترونية مخزنة على كارت ذكي أو قرص صلب بحيث يستطيع صاحبها نقل ملكيتها إلى من يشاء دون تدخل شخص ثالث**»[1].

كما عرفها الأستاذ "محمد إبراهيم محمود الشافعي" أنّها «قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدما وغير مرتبطة بحساب بنكي، وتحظى بقبول واسع من غير من قام بإصدارها وتستعمل كأداة للدفع لأغراض مختلفة»[2].

فالنقود الرقمية عبارة عن منتجات دفع متنوعة مخصصة للمستهلك تستخدم لدفع المستحقات بطرق الكترونية بدلا من استخدام الوسائل التقليدية[3]، واعتمادا على المقاربات التي أشرنا إليها يمكننا الاستنتاج أن النقود الإلكترونية حقيقة قانونية على المستوى الأوروبي وهذا بتكريسها في النصوص القانونية، أما على المستوى العربي تبقى وهم

1- **هيثم عدنان عزو**، النقود الإلكترونية، مقال منشور على الموقع : http://www.arabe-law.com

2- **محمد إبراهيم محمود الشافعي**، النقود الإلكترونية (ماهيتها، مخاطرها وتنظيمها القانوني)، مجلة الأمن والقانون، دبي، العدد الأول جانفي 2004، مقال منشور على الموقع http://www.mostathmr.com/vb/t12223.html

3- **جلال عايد الشورى**، وسائل الدفع الإلكترونية، دار الثقافة للنشر والتوزيع، طبعة أولى، 2008، ص57.

اقتصادي وذلك لعدم النص عليها في التشريعات العربية، وهذه نتيجة منطقية للفرق الموجود بين هذه الدول من حيث التطور التشريعي الذي يعاكس التقدم والتطور التكنولوجي.

ثانيا- خصائص النقود الرقمية:

لقد سبق الإشارة إلى أن النقود الإلكترونية عبارة عن مخزون لقيمة نقدية تكون محفوظة بشكل رقمي (Digital forme) وتتميز بالكثير من الخصائص.

1- قيمة نقدية:

بالرغم من الطابع الإلكتروني لهذه الوحدات المستخدمة في الدفع إلاّ أنّها تمثل قيمة مالية وتشبه فعلا النقود العادية، مع فارق وحيد هو أنه بدل أن تكون في صورة ورقية أو معدنية، فهي في صورة لا مادية غير ملموسة يتم تداولها بشكل إلكتروني، وتبقى صالحة كأداة وفاء في المشتريات العادية البسيطة واليومية التي يقوم بها المستهلكون عبر الإنترنت.

2- سهلة وسريعة التحويل:

- تحتفظ النقود الإلكترونية بقيمتها باعتبارها معلومات رقمية مستقلة عن أي حساب أخر.
- تحويل قيمة النقود الإلكترونية إلى أي شخص وذلك عن طريق تحويل المعلومات الرقمية إمكانية تحويل هذه النقود عن طريق الشبكات مثل الإنترنت أو الشبكات الاتصال اللاسلكية أخرى.
- سهولة استخدامها مقارنة مع وسائل الدفع الأخرى، لذا تشجع المستهلك على استخدامها، ويكون قبول نظامها ضمان لاستمرار حياة هذه النقود باستعمالها الدائم.
- تستخدم في أي وقت تماشيا مع طبيعة الإنترنت وما تقتضيه طبيعة التجارة الدولية لاختلاف الأوقات بين الدول[1].

1 - **جلال عايد الشورى،** وسائل الدفع الإلكترونية، المرجع السابق، ص69.

يمكن إعادة استخدام شهادة النقود الرقمية(*) مرات متعددة، حيث لا يوجد ما يحول دون أن يقوم البائع الذي تلقاها باستخدامها في الوفاء بالالتزامات النقدية لصالح بائع أو أي دائن أخر [1].

بالرغم من الطابع الإلكتروني لهذه الوحدات المستخدمة في الدفع إلاّ أنّها تمثل قيمة مالية وتشبه فعلا النقود العادية، مع فارق وحيد هو أنه بدل أن تكون في صورة ورقية أو معدنية، فهي في صورة لا مادية غير ملموسة يتم تداولها بشكل إلكتروني، وتبقى صالحة كأداة وفاء في المشتريات العادية البسيطة واليومية التي يقوم بها المستهلكون عبر الإنترنت.

3- أداة وفاء:

تصدر النقود الإلكترونية لغرض واحد وهو دفع وسداد قيمة المشتريات وتصدر خصيصا لهذا الغرض، بحيث لم تكن موجودة قبل ذلك على عكس النقود العادية، وبالتالي هي مؤقتة بعملية الدفع، بحيث إذا ما تمت عملية الدفع تحولت إلى مصدرها وتصبح نقودا عادية، ولا تبقى في صورتها الرقمية وإنما يتم استردادها لحالتها العادية كنقود عادية. بمعنى هي عملية تحويل للنقود العادية مؤقتا إلى صورة رقمية للقيام بعمليات معينة وبمجرد انتهائها تعاد العملية العكسية وترجع إلى طبيعتها.

*- النقود الرقمية إذن هي نظام لسداد المستحقات بتحويل رقم فريد أو مجموعة أرقام (أي غير قابلة للتكـ ـرار..) من كمبيوتر المدين إلى كمبيوتر الدائن وتبدأ معظم نظم النقود الالكترونية ببنك مشترك في إصدار مثل هذه النقود أي أرقام دالة على مبلغ معين، وللحصول أي شخص على هذه الأرقام أو بالأحرى الشهادة التي تحمل هذه الأرقام من البنك يجب أن تكون له حساب لدى هذا البنك.

وعندما تشتري شهادات النقد الرقمي يقوم البنك بسحب المبلغ المقابل من حسابك لديه ، وعندما تبلغ هذه الشهادة (أي تبلغ أرقامها) إلى البائع أو إلى أي شخص آخر دائن لك فيقوم بدوره بإيداع هذه النقود لدى أي بنك مشارك في نظام النقد الرقمي، كما يمكنه أن يعيد استخدامها على سداد التزاماته قبل الدائنين له، وغالبا ما يقوم الدائن بالاتصال بالبنك المصدر لهذه النقود للاطمئنان من صحة الشهادات الخاصة بها، لاسيما في حالة المشتريات عالية القيمة.

1 - **إبراهيم العيسوي**، التجارة الالكترونية، المكتبة الأكاديمية، مصر، ط1، 2003، ص87.

4 - ذات طبيعة دولية غير مادية:

وهي صفة لصيقة بطبيعة العملية التي وجدت خصيصا لها وهي التجارة الإلكترونية وعقودها المتسمة بالطابع الدولي عموما، وهي غير مادية، كونها مشكلة من متتاليات رقمية مشكلة من رقمي |0| و|1|، لكن طبيعتها الدولية لا تعني أنّها أصبحت من العملات الصعبة[1].

ويرى الاقتصاديون أنه لكي نكيف العملة بأنها دولية، حينما يتم اعتمادها من طرف عدد كبير من الدول، وتستعمل كوسيلة وفاء في منطقة تتعدى حدود الدولة التي أصدرتها[2].

نستنتج إذن أن هذا التكييف يتماشى مع طبيعة النقود الالكترونية، التي تتعدى حدود استعمالها حدود الدولة المصدرة بإمكانية استعمالها عبر الشبكة العنكبوتية.

5- تمتعها بالأمان والسرية:

يهدد التزام الوفاء عن بعد عبر فضاء دولي مفتوح باستعمال النقود الإلكترونية عدة مخاطر، لذا يجب أن تكون بوسائل أمان تضفي الثقة للتعامل بها، باعتبار وجودها جد آمن ويستحيل ضياع القيمة النقدية التي تمثلها البطاقة، بالإضافة إلى ما توفره من خفض تكلفة العملية المصرفية وتوفير عدد كبير من الموظفين، وسهولة حملها عند التسوق.

1- ويرى الدكتور حمودي ناصر أنه تبقى قيمة النقود الإلكترونية زهيدة لا تلاءم قيمة ما يمثله الثمن في عقد البيع الدولي للبضائع، حيث تم استبعاد هذه العقود بموجب أحكام اتفاقية فينا للبيع الدولي للبضائع.

أنظر: حمودي ناصر، النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنت، رسالة لنيل درجة دكتوراه في القانون، جامعة مولود معمري، تيزي وزو، 2009، ص 385.

2 -Une monnaie deviendra monnaie internationale, d'une part, elle sera adoptée par un grand nombre D'Etats comme monnaie de rattachement et de libellé pour les avoirs de change(internationalisation officielle) et lorsque , par ailleurs elle sera utilisée comme monnaie de règlement et de facturation dans une zone qui dépasse les frontières de la nation émettrice voir : **BOUKELLA (M.), BENABDALLAH (Y.), FERFERA (M.Y.)**, La méditerrané occidentale, entre régionalisation et mondialisation, édition CREAD, université Abderrahmane mira, Bejaïa, 2000, p.134.

كلها مؤشرات جعلت البعض يرى بأن النقود الورقية سوف لن تصمد طويلا أما النقود الإلكترونية وقد تختفي من التعامل على المدى البعيد. وحسب تقدير الدكتور "حمودي ناصر" أن ذلك سيكون على المستوى المحلي في التعاملات البسيطة على الأقل في الوقت الراهن.

وبالإضافة لما سبق ذكره فإن النقود الإلكترونية تتمتع بالعديد من الخصائص الأخرى، والتي كثرت بسبب اختلاف الفقه في زاوية دراستها وطريقة تناولها، وهو الأمر الذي انعكس كما سبق القول على تسميتها وتعريفها وحتى حصر خصائصها بدقة.

فنجد من قال بأن النقود الإلكترونية تتمتع أيضا، مثلما تدل عليه تسميتها، بخاصية أنها قيمة مخزنة على وسيط إلكتروني. مما يجعلها فنيا عبارة عن إشارات يرسلها الكمبيوتر المثبت على كارت المستهلك إلى الكمبيوتر المثبت على كارت التاجر ويتم دفع قيمتها مسبقا من قبل الشركات المصدرة لها.

بالإضافة إلى خاصية ساهمت كثيرا في انتشارها وهي عدم ارتباطها بحساب بنكي، بحيث أن حاملها لا يحتاج لفتح حساب حتى يتزود بها بل هي محمولة على بطاقات بحوزته يحملها أينما حلّ، هذا بالإضافة إلى كونها نقود تتميز عن غيرها من وسائل الدفع، وأهم هذه الخصائص أنها تلعب دور الوسيط في عملية التبادل كونها نقودا قابلة للتحويل في أي وقت إلى نقود حقيقية كونها مجرد وسيط في المعاملات التي تتم عبر الإنترنت ليستكمل العمل بالنقود الحقيقية العادية بالإضافة إلى أنّها نقود غير متجانسة كونها تصدر بفئات مالية مختلفة كل فئة يعبر عنها برقم معين، سواء من ناحية قيمتها أو من ناحية ما يمكن أن يتم استيفاؤه بها، أو حتى بحسب الجهة المصدرة لها.

وهي بذلك ليست نقودا متجانسة بل تختلف من نوع لأخر من أنواعها أو من مستهلك لأخر بحسب ما حمله في محفظته أو حاملة نقوده وهي الأمور كلها التي تجعلها تتميز بسهولة الحمل والاستخدام كون إصدارها يراعي فيه اعتبارات الملائمة من حيث حملها واستخدامها السهل والحفظ والنقل، كونها تدار بواسطة برمجيات بسيطة تحتاج إلى

قدر متواضع من متطلبات التشغيل سواء من جهة المعدات أو البرمجيات، وهي أمور كلها تجعل منها حقيبة نقود من نوع خاص لم يسبق للعالم أن كان له عهد بنظير لها[1].

6 - يمكن أن تصدرها المؤسسات الخاصة:

على عكس النقود القانونية التقليدية التي يتم إصدارها والتحكم في كمها وشكلها من طرف البنك المركزي في كل دولة فإن النقود الإلكترونية يتم إصدارها في غالبية الدول عن طريق شركات خاصة أو مؤسسات ائتمانية خاصة ومختصة في هذا المجال، ولهذا يطلق على هذه النقود اسم "النقود الخاصة"[2].

ويمكننا القول أنها وسيلة تتلاءم وطبيعة التجارة الإلكترونية التي تتم بواسطة تكنولوجيات الاتصالات الحديثة والتي تجرد المعاملات من طابعها المادي، فتكون النقود الإلكترونية تستجيب لما يسعى هذا النوع من التجارة في عالم المعالجة الإلكترونية للبيانات واستغلالها في المعاملات التجارية.

الفرع الثالث

التعرف على هوية أطراف عملية الدفع الإلكتروني

يكمن جوهر التصرفات القانونية في ضرورة تعرف أطراف العلاقة القانونية بعضها البعض بالحضور الفعلي لدى التعاقد، وهو الشرط الذي لا يتحقق عن الدفع الإلكتروني بنقل البيانات بين المعاملين وغياب مجلس العقد بعدم الحضور الجسدي لأطراف العقد الشيء الذي يفسح المجال لمضاعفة محاولات الاعتداء والسطو على ممتلكات الغير، من خلال القرصنة الإلكترونية، سرقة البيانات والاستعمال غير المشروع لوسائل الدفع الالكترونية.

1- **حمودي ناصر،** النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنت، المرجع السابق، ص386-387.

2- **محمد إبراهيم محمود الشافعي،** الآثار النقدية والاقتصادية والمالية للنقود الإلكترونية، بحث مقدم في مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي 10 و12 ماي 2003، ص140 منشور على الموقع : http://slconf.uaeu.ac.ae

وللتقليل من مخاطر هذه العملية وبعث الثقة والضمان بين المتعاملين، تم استعمال وسيلة التوقيع الإلكتروني الذي يعبر عن هوية الطرف الذي يريد نقل مبلغ من نقوده الإلكترونية إلى الدائن، من هنا ظهرت الحاجة الملحة إلى ضرورة إيجاد بديل الكتروني يحل محل التوقيع الخطي اليدوي ويؤدي نفس وظائفه من حيث التوثيق والإثبات كما يمنع المرسل من إنكار المعلومات التي أرسلها (Non répudiation).

أولا- تعريف التوقيع الإلكتروني:

عرف المشرع المصري التوقيع الإلكتروني في القانون رقم 2004/10 في المادة الأولى أنه «***ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح تحديد شخص الموقع ويميزه عن غيره***»[1].

كما عرف قانون الأونسيترال النموذجي للتوقيع الإلكتروني سنة 2001 التوقيع الإلكتروني في المادة الأولى بأنّه «***بيانات في شكل الكتروني مدرجة على رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، ويجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة بيانات ولبيان موافقة الموقع على المعلومات الواردة فيها***»[2].

أما القانون الفدرالي(الأمريكي) يعرفه على أن التوقيع الإلكتروني «***أي رمز أو وسيلة بصرف النظر عن التقنية المستخدمة إذا ما تم نسبه إلى شخص أخر يرغب على توقيع مستند***»[3].

كما يعرفه بعض الفقه أن التوقيع الإلكتروني هو استعمال تشفير ذات المفتاح العام "فيفترض أن يكون لكل مستعمل لهذه التقنية مفتاح خاص ومفتاح عام، فتكون الإشارات

---

1 - **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص191.

2 - **وائل أنور بندق**، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، المرجع السابق، ص103.

أنظر في ذلك نص المادة الأولى من قانون الاونسيترال النموذجي بشأن التوقيعات الإلكترونية 2001.

3 - **خالد ممدوح إبراهيم**، المرجع السابق، ص191.

على شكل كلمة سر يتم تبيانها عن طريق برنامج الكمبيوتر الذي يتأكد بان هذه الكلمة التي تعبر عن المفتاح السري للشخص هي حقا توقيع مرسل البيانات[1].

ثانيا- التوقيع الإلكتروني في الجزائر:

إن الكتابة والتوقيع الإلكترونيين سيعرفان تطبيق واعد في الجزائر وهذا بفضل تعديل القانون المدني الذي تم في ماي 2005، ويظهر ذلك في تعديل المواد 323 مكرر1 والتي تنص صراحة: «***يعتبر الإثبات بالشكل الإلكتروني كالاثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها***»[2] وحسب تقدير بعض المسؤولين فإنّه ينتظر المراسيم التنفيذية التي تبين مجال التطبيق الدقيق لهذه النصوص، حيث أنّه لا يعطي أية حرية أو سلطة تقديرية في تفسير هذه النصوص[3].

لذاك على الجزائر أن تضع حيز التنفيذ هذه النصوص في اقرب وقت ممكن وذلك قصد إعطاء الدفع للمبادلات الإلكترونية والتجارة الإلكترونية بأكملها وكذلك بدعم مفهوم العمل الإلكتروني الموقع خاصة وأن معظم المبادلات التجارية الجزائرية تتم مع الاتحاد الأوروبي هذا الأخير الذي يعرف استعمال كثيرا من المستندات الالكترونية في معاملاته خاصة منذ 2002[4].

ويرى السيد "موني" Monnier المختص في الإعلام الآلي على الدور الفعال الذي تلعبه الكتابة الإلكترونية في تطوير التجارة الخارجية لأي بلد.

1- Peut décoder la signature numérique à partir de la clé publique, Le système suppose tout d'abord que la clé publique soit comme par le destination , lors de la réception du message de système va Vérifier automatiquement s'il dispose de la clé publique de l'auteur de message. Voir : **WERY Etienne**, Facture, Monnaie, op.cit, p.51.

2- المادة323 مكرر1 من القانون المدني الجزائري، التي تضمنها القانون رقم 05-10 مؤرخ في20 يونيو 2005.

3- Déclaration de **GUESSOUM Fouzia**, In www.jeuneindipendant.com, jeudi 5 Mai 2005.

4- **BOUAISSA Karim**, Le commerce et la vague Internet, Mémoire de licence en Management faculté des sciences de gestion, Laghouat, Algérie, publié sur site : www.memoireonline.com.

ثالثا: حجية التوقيع الإلكتروني:

يعبر التوقيع في شكله الكتابي التقليدي دليلا على نية الموقع والإقرار بتحريره نص المستند، وأيضا كدليل للإثبات وأداة للتعبير عن إرادة الشخص على قبوله الالتزام بمضمون العقد ووسيلة من تأمين العقد من التعديل.

يتفوق التوقيع الإلكتروني على التوقيع التقليدي بالنظر للاستياق مع شخصية صاحب التوقيع، يتم بشكل روتيني في كل مرة يتعامل فيها بالمحررات الإلكترونية باستخدام الرقم السري أو المفتاح الخاص بالتالي لا مجال للانتظار، حتى ينشب النزاع للبحث في مدى صحة التوقيع ، أضف إلى ذلك ما توفره التقنية الحديثة المستخدمة في تأمين التوقيع الإلكتروني عن طريق ما يسمى نظام المعاملات الإلكترونية الآمنة. حيث يوفر هذا النظام التحقق من شخصية الموقع(1).

الفرع الرابع

زمان ومكان تنفيذ الالتزام بالدفع الإلكتروني

عدلت البيئة الإلكترونية كثيرا وأحيانا بطريقة جذرية القواعد العامة التي كانت تحكم زمان ومكان أداء الثمن من المشتري للبائع أو من يمثله. أين أصبح المشتري يتمتع بهامش ضيق في اختيار طريقة الدفع وزمام ومكان الوفاء بالالتزام، بحيث أصبح في العادة البائع يفرض ذلك مسبقا.

أولا- زمان تنفيذ الالتزام بالدفع:

تلزم اتفاقية فيينا للبيع الدولي للبضائع المشتري بدفع الثمن في الميعاد المحدد في العقد أو الذي يمكن تحديده بالرجوع إليه، ولا تطبق أحكام الاتفاقية إلا إذ خلا العقد من بيان كيفية تعيين هذا الميعاد. وقد وضعت الاتفاقية قاعدة أساسية ربطت فيها بين ميعاد دفع الثمن وميعاد التسليم، وإن لم يكن المشتري ملزم بدفع الثمن في وقت محدد، وجب

1- **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، المرجع السابق، ص193.

عليه أن يدفعه عندما يضع البائع البضائع أو المستندات التي تمثلها تحت تصرف المشتري وفقا للعقد (وفقا لنص المادة 1/58 منها)[1].

فيجوز للبائع أن يعتبر الدفع شرطا لتسليم البضائع أو المستندات. فلا تسلم إلا بعد دفع الثمن، ويجب على المشتري الوفاء بالثمن بمجرد حلول ميعاد الوفاء به دون حاجة إلى قيام البائع بتوجيه أي طلب أو استيفاء أي إجراء.

غير أن ما أفرزته التجارة الإلكترونية من تطورات أو تطبيقات جديدة، غيرت هذه القاعدة بطريقة جد حساسة، بحيث نادرا ما نجد الدفع في عقود البيع الإلكترونية قد تم خارج وقت إبرامه، وعادة ما لا يتم التنفيذ إلا بعد الدفع باعتبار البائع هو الذي يحدد ذلك لاسيما في العقود التي تتم عبر مواقع الويب، أين ينفرد البائع بوضع مثل هذا الشرط قبل توريده أو قبل تسليمه للشيء. ويرى البعض أنه يستحسن عدم الدفع في العقود الإلكترونية قبل التسليم خوفا من أن لا ينفذ البائع التزامه بعد قبض الثمن، بالإضافة لما تتميز به طرق الدفع في البيئة الرقمية من تعقيد.

فمن المستحسن ترك الحرية للأفراد لتنظيم المسالة تماشيا مع حاجاتهم ومقتضيات التجارة الإلكترونية وحتى التجارة الدولية التقليدية، أين جعلت اتفاقية فينا ذاتها من قواعدها قواعد مكملة يجوز للأطراف الاتفاق على غير ما نصت عليه أو استبدالها، فإنّه يحسن ترك الحرية للأفراد في تحديد زمان تنفيذ المشتري لالتزامه بالدفع سواء قبل أو بعد التسليم[2].

ثانيا- مكان تنفيذ الالتزام بالدفع:

طبقا لنص المادة 57 من اتفاقية فيينا سالفة الذكر، يلتزم المشتري بدفع الثمن في المكان المتفق عليه في العقد وإن غفل على تحديد ذلك وجب على المشتري أن يدفعه في مكان عمل البائع حسب المادة نفسها[3].

1- اتفاقية فيينا بشأن عقود البيع الدولي للبضائع المعتمدة في المؤتمر الديبلوماسي في 11 افريل 1980 والتي دخلت حيز النفاذ في 1 يناير 1988 منشورة على الموقع www.unicitral.org

2- **حمودي ناصر،** النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنت، المرجع السابق، ص391-392.

3- والعبرة هنا بمكان عمل البائع وقت عملية الدفع لا وقت إبرام العقد. أنظر: المرجع نفسه، ص392.

ونتساءل عن كيفية تحديد مكان الدفع الإلكتروني في بيئة الكترونية غير مادية ودولية التي يصعب فيها تحديد مكان تواجد الطرفين المتعاقدين، ويمكن القول بصفة عامة أن مكان الدفع متروك لإرادة الطرفين المتعاقدين، وفي حالة غياب اختيارهم فإن مكان الدفع متروك للقواعد العامة التي تحدد ذلك في القانون الداخلي المطبق على العقد.

خاصة وأن مسألة تحديد مكان الدفع تعد من المسائل الجد مهمة بالنسبة لهذا النوع من العقود كون المكان هو الذي يحدد عملة الدفع إن لم تكن بطرق إلكترونية، غير أن التطبيقات والممارسات العملية للتجارة الإلكترونية جرت على تحديد مكان الدفع بالمكان الذي يتواجد فيه موزع الإنترنت الخاص بالموجب لما يكون العقد قد أبرم على موقع من مواقع الإنترنت. ونفس الشيء بالنسبة للعقود المبرمة عبر البريد الإلكتروني فإن المكان الذي يوجد به الموجب. وعملة الوفاء في الغالب تكون العملة المتداولة في الدولة التي يتواجد بها غالبية نشاطات التاجر وأحيانا عملة العقد هي التي تحدد وتكون معيارا لتحديد المكان[1].

1- **حمودي ناصر،** النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنت، المرجع السابق، ص393.

المبحث الثاني
وسائل الدفع الإلكترونية المطورة والحديثة

نتج عن التطور الذي جاءت به التجارة الإلكترونية، وسائل عديدة يتم بموجبها تنفيذ العقود والالتزامات المترتبة عن العلاقات القانونية التجارية من بيع سلع وتقديم خدمات عبر الانترنت، وكنتيجة منطقية لذلك، ظهرت عدة وسائل دفع، يتم بموجبها انقضاء التزام المشتري بالوفاء بالثمن.

ويمكننا التمييز في هذا الصدد بين نوعين من وسائل الدفع، منها ما كان موجودا وما تغير فيها إلا طرق معالجتها، منها السفتجة الورقية، والشيك الورقي العادي، اللذين يعتبران وسيلتين للوفاء وتعبيرا لإرادة الطرفين على دعامة ورقية في شكلها التقليدي فمعالجتها إلكترونيا يعطيها صبغة تتماشى وطبيعة التجارة الإلكترونية.

لذا ارتأينا إلى دراسة الوسائل في شكلها الحديث فقط التي تغيرت طريقة معالجتها وطرق تداولها، فبعدما كانت على دعائم ورقية كما سبق وأن ذكرنا، أصبحت التجارة الإلكترونية تحتاج إلى هذه الوسائل، شرط أن تتماشى وطبيعتها، فندرس الوسائل المطورة منها السفتجة الإلكترونية والشيك الإلكتروني (مطلب أول).

لم يتوقف تطور التجارة الإلكترونية عند هذا الحد، بل تم اختراع وسائل جديدة وليدة التطور التكنولوجي نفسه واحتياجات التجارة الإلكترونية أيضا، فظهر ما يسمى بالنقود البلاستكية على شكل كروت معبأة بوحدات نقدية إلكترونية، والتي تتعدد أنواعها حسب غرض إصدارها، وهذه الكروت أو البطاقات البنكية نتج عنها نظام دفع معقد كل بحسب التزاماته وحقوقه، حيث يختفي فيها دور الورق تماما، ويتم بشكل كلي من خلال الوسائط الإلكترونية، فتصدر من البداية على دعامة الكترونية ممغنطة، وإذا حدث تداول

يتم تداولها أيضا من خلال وسائل الكترونية[1]، لذلك ارتأينا دراسة هذه الوسائل في (مطلب ثاني).

ويتم بموجب الوسائل المطورة أو المستحدثة على حد سواء، تحويل النقود الكترونيا، وهذا ما يسمى بالتحويل المصرفي الإلكتروني، الذي يتم بين المؤسسات المالية المتمثلة في البنوك أو المؤسسات المصدرة لخدمات وسائل الدفع الإلكتروني. لذا سنتولى دراسة هذا النوع من التحويل كونه من أهم العمليات المصرفية وأوسعها انتشارا بين المؤسسات المالية حديثا (مطلب ثالث).

المطلب الأول

وسائل الدفع الإلكترونية المطورة

من خلال التسمية، يظهر لنا جليا أن الدراسة ستنحصر حول وسائل كانت موجودة من قبل، ولم يتغير فيها سوى طريقة معالجتها وتداولها، حيث أنّها استعملت على دعائم ورقية في التجارة التقليدية [2]، فيتم دراسة السفتجة الإلكترونية (فرع أول)، ولعل الوسيلة الأكثر استعمالا وتداولا هو الشيك الورقي الذي تم تطويره هو الأخر بمعالجتها الكترونيا كذلك، وهذا ما يسمى بالشيك الإلكتروني (فرع ثان).

الفرع الأول

السفتجة الإلكترونية نظيرة للسفتجة الورقية

تعتبر السفتجة في شكلها العادي محررة على دعامة ورقية، عملا تجاريا حسب الشكل ووسيلة دفع، وتتضمن لصحتها الشروط الواردة في نص المادة 390 من القانون التجاري الجزائري المتمثلة في:

1- **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، المرجع السابق ص343.

2- **محمد عمر ذوابة، أكرم مالكي**، عقد التحويل المصرفي الالكتروني (دراسة قانونية مقارنة)، دار الثقافة للنشر والتوزيع، دون بلد النشر، 2006، ص9.

- تسمية "سفتجة" في متن السند نفسه وباللّغة المستعملة في تحريره.
- أمر غير معلق على قيد أو شرط بدفع مبلغ معين.
- اسم من يجب عليه الدفع (المسحوب عليه).
- تاريخ الاستحقاق.
- المكان الذي يجب فيه الدفع.
- اسم من يجب الدفع له أو لأمره .
- بيان تاريخ أنشاء السفتجة ومكانه.
- توقيع من أصدر السفتجة (الساحب)[1].

وفي وقتنا الحالي، أغلبية السفتجات المحررة يتم معالجتها الكترونيا، وهذا باستعمال الدعائم الإلكترونية عوض الدعائم الورقية [2].

أولا- ماهية السفتجة الإلكترونية:

ترتبط نشأة السفتجة الإلكترونية بالتجربة الفرنسية، نتيجة لجهود اللجان التي اضطلعت بمحاولة حل المشاكل المالية والإدارية الناشئة عن التعامل بهذه الوسيلة، خاصة إذا ما تعلق الأمر بتدخل البنوك كطرف في هذه المعاملة، ورغبة في الاستفادة من تقنيات المعلوماتية الحديثة والتجهيز الإلكتروني، خاصة في ظل وجود الحاسب الآلي للمقاصة الموجود بالبنك المركزي بفرنسا[3] مثلا.

ويرجع تاريخ بدء العمل بالسفتجة الإلكترونية إلى 02 جويلية سنة 1983، فهي ثمرة جهود لجنة (Gillet) المتعلقة بتخفيض ائتمان قصير الآجل، ولعل نشأة الكمبيالة

1- المادة 390 من القانون التجاري الجزائري، في ضوء الممارسات القضائية الجديدة، منشورات بيرتي 2010/1/2009، الجزائر، ص134.

2- Aujourd'hui la quasi-totalité des lettres de change sont émises sous la forme informatique de Lettre de Change Relevée (L.C.R) dans le cas de l'utilisation sous forme électronique. Voir : **TOERING Jean Pierre et BRION François,** les moyens de payements, op.cit, p73 .

3- **مصطفى كمال طه، وائل أنور بندق،** الأوراق التجارية وسائل الدفع الالكترونية الحديثة، المرجع السابق، ص345.

الإلكترونية في رحاب البنوك بهذه الصورة هي التي جعلت من التجربة الفرنسية نبراساً للفقهاء الذين تعرضوا لدراسات للأوراق التجارية الإلكترونية[1].

1- تعريف السفتجة الإلكترونية:

لا يختلف كثيرا تعريف الكمبيالة الإلكترونية عن مثيلتها المحررة على الدعائم الورقية، فنظام الكمبيالة الإلكترونية يعتمد على تدقيق أو تطوير للنظام أو الميكانيزم الذي وضع للكمبيالة الورقية [2].

فيمكن القول أن السفتجة الإلكترونية عبارة «عن محرر شكلي، ثلاثي الأطراف معالج الكترونيا، بصورة كلية أو جزئية، يتضمن أمراً من شخص يسمى الساحب إلى شخص أخر يسمى المسحوب عليه بأن يدفع مبلغا من النقود لشخص ثالث يسمى المستفيد لدى الاطلاع أو في تاريخ معين».

والواقع أنّه ليس هناك ما يمنع من الناحية القانونية أن توجد الكمبيالة الإلكترونية فيما بين الأفراد والشركات مع بعضها البعض، من خلال الشبكات الخاصة، بل ومن خلال شبكة الإنترنت. إلى جانب استعمالها في العمليات المصرفية، فهي عملية تعتمد على قدر كبير من التنظيم الفني والقانوني لمثل هذه الفروض، خاصة في ضوء الاعتراف بحجية المستندات الإلكترونية، ووجود طرف ثالث، مثل هيئات التصديق الإلكتروني التي تضمن الثقة والمصداقية لدى الأطراف المتعاملة بالكمبيالة الإلكترونية[3].

1- ولا تزال الدراسات المتعلقة بالأوراق التجارية الالكترونية ضئيلة، فلم يصدر منها في الفقه العربي بالكامل إلاّ ثلاثة مؤلفات تناولت الوفاء بالأوراق المعالجة الكترونيا. أنظر: **محمد بهجت عبد ا قايد،** الأوراق التجارية الالكترونية، دار النهضة العربية، مصر، دون تاريخ النشر، ص7.

2-«En effet le droit cambiaire résultant des conventions de Genève repose sur l'exigence absolue d'un titre papier qui sert de support …or c'est précisément ce support qui est supprimé dans la lettre de change relevé magnétique… ». Voir : **JEANTIN Michel, PAUL Le Cannu**, Droit commercial: instruments de paiement et de Crédit, entreprise en difficulté, 5ème édition, Dalloz, Paris, 1999, pp276-277.

3- **مصطفى كمال طه، وائل أنور بندق،** الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، المرجع السابق ص346.

2- أنواع السفتجة الإلكترونية:

ظهر نوعين أساسيين من الكمبيالات الالكترونية فيمكننا التمييز بين:

أ- السفتجة الورقية أو المقترنة بكشف (La lettre de change relevé papier):
ويرمز لها اختصارا بـ (L.C.R Papier)، وهي التي تصدر من البداية في شكلها التقليدي على دعامة ورقية، ثم يتم معالجتها الكترونيا عند تقديمها لدى البنك لتحصيلها أو بمناسبة تظهيرها لأي طرف آخر.

فيكون لها شكلية إلكترونية بواسطة بيانات تتداول عبر قنوات الاتصال بين حواسيب الأطراف المتعاملة بها.

ب- السفتجة الممغنطة(La lettre de change relevé magnétique): و التي لا تعتبر عملا تجاريا يرمز لها اختصارا بـ (L.C.R Magnétique)، وفي هذا النوع يختفي أصلا أي ظهور للدعامة الورقية، تصدر من البداية على دعامة ممغنطة مستوفية لكافة البيانات اللازمة لصحتها الخاصة بالمستفيد، المسحوب وتوقيع إلكتروني. والواقع أن هذا النوع هو الذي يمثل قمة الاستفادة من التقنيات الإلكترونية الحديثة[1]، فتحرر وتتداول في كل مراحلها بالطرق الإلكترونية.

3- الطبيعة القانونية للسفتجة الإلكترونية:

تضاربت الآراء في هذا المقام حول طبيعة الكمبيالة الإلكترونية، فيما إذا كانت عملا تجاريا حول القواعد التي تخضع لها والتي ندرسها في النقاط التالية:

أ- السفتجة الإلكترونية ليست عمل تجاري؟: اعتبر اتجاه من الفقه السفتجة الإلكترونية ليست عملا تجاريا، ولا تعبر عن تسميتها، أي أنّها ليست السفتجة، ولذلك فإن قانون الصرف الذي نتج عن اتفاقيات جنيف يعتمد على الحتمية المطلقة على وجود أمر على دعامة ورقية، والذي يحمل الشروط الشكلية المذكورة سالفا، والشيء ذاته يظهر على

1- **مصطفى كمال طه، وائل أنور بندق،** الأوراق التجارية وسائل الدفع الالكترونية الحديثة، المرجع السابق، ص346.

الدعامة الورقية لكن يغيب ولا تظهر تماما في السفتجة الإلكترونية فتكييفها أنّها سفتجة مستبعدة بالضرورة.

وكنتيجة لذلك لا يتم تطبيق قواعد القانون التجاري[1] على هذه الوسيلة من وسائل الدفع الإلكترونية، وبالتالي لا يمكن أن تكون محل نفس قواعد الكمبيالة العادية كالتظهير ونقل الملكية والقبول، ومن المستحسن أن تكون إجراءات الكمبيالة الإلكترونية أقرب إلى تلك الخاصة بالكمبيالة الورقية، فكل قواعد قانون (Cambiaire) مستبعـدة خاصة القواعد الخاصة بالطابع الإلزامي لميعاد الدفع الذي لا يسمح بأي ميعاد إضافي[2].

ب-خضوع السفتجة الإلكترونية للقواعد العامة الخاصة بالحوالة: ويرى هذا الاتجاه وعلى رأسهم الأستاذ "فاسور" M. Vasseur، حيث قال أن الكمبيالة الإلكترونية تخضع لنظام يقترب من النظام الذي يخضع له أمر الدفع (Avis de prélèvement) فالبنك الذي يدفع بمناسبة كمبيالة الكترونية، يقوم بخصم المبلغ من رصيد زبونه (صاحب الرصيد)، بعدما يقوم هذا الأخير بالسماح بهذا الخصم عن طريق أمر الدفع لصالح المستفيد.

واعتمادا على ذلك، فإن تقنية الحوالة تشترك في الكمبيالة الإلكترونية على مستويين:

- عن طريق المسحوب عليه (Le tiré) الذي تسحب عليه الكمبيالة الإلكترونية (L.C.R Magnétique) والذي يقدم للبنك أمرا لإجراء الدفع، أي الدفع بموجب أمر الكمبيالة الإلكترونية.
- عن طريق المدين عندما يأمر البنك عند إرجاع الأمر (Le relevé) أو الكمبيالات الإلكترونية، ويؤكد على عملية الدفع.

فتتم عملية الدفع بتحويل مبلغ الكمبيالة من رصيد المدين إلى رصيد الدائن، وفي كل الأحوال لا يمكن اعتبار الشريط المغناطيسي يمثل طبيعة الدين، فما هي إلاّ وسيلة

1-**JEANTIN Michel**, Droit commercial: instruments de paiement et de Crédit , entreprise en difficulté, 4ème éditions, 2005, p.264.

2-Ibid, p.264.

إثباته. ويمكننا استنتاج البعد الذي يفرق بين الكمبيالة الإلكترونية (L.C.R Magnétique) والأعمال التجارية، إذا كانت ضمانات دفع هذا الأخير نتيجة قطعية لالتزامات الموقعين. بالتالي فإن ضمانات دفع الكمبيالة الإلكترونية تعتمد أساسا على العلاقة التعاقدية والائتمان بين البنك وزبونه[1].

وعلى ذلك لا مناص من اللجوء إلى القواعد العامة التي وضعها المشرع للأوراق التجارية التقليدية التي أدرج الفقه تسميتها بقانون الصرف، وفي رحاب هذه القواعد يثور التساؤل عن مدى خضوع الكمبيالة الإلكترونية بنوعيها لقانون الصرف. فإجابة الفقه عن هذا السؤال انطلقت من نظرة مبدئية وهي ضرورة المحرر الورقي كمحرر لتطبيق أحكام قانون الصرف، ومن ثم كانت الإجابة البديهية أن الكمبيالة الإلكترونية الورقية تخضع لأحكام قانون الصرف، أما الممغنطة فلا يمكن أن تخضع لأحكام هذا القانون[2].

ج- حجية السفتجة الإلكترونية: الواقع أن ما تم تحليله سابقا في عنصر طبيعة الكمبيالة الالكترونية محل نظر ودراسة، خاصة بعد صدور قانون التوقيع الإلكترونـي ذلك أن المشرع لم يشترط في المحرر أن يكون ورقيا، فلا توجد في الأصل اللّغوي لكلمة المحرر ما يقتصر معناه على ما هو مكتوب على نوع معين من الدعامات، سواء كان ورقيا أو غير ذلك، لذلك يمكن القول أن كلمة محرر تشمل المحرر الكتابي والإلكتروني على حد سواء[3].

1- **JEANTIN Michel**, Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, 4ème éditions, 2005, p265.

2- وأول ما يلاحظ في هذا الصدد هو غياب تنظيم قانوني متكامل لفكرة الأوراق التجارية الالكترونية، سواء على الصعيد الداخلي أو الدولي، صحيح أنه قد صدرت العديد من القوانين المتعلقة بالتجارة الالكترونية، والتوقيع الالكتروني، إلاّ أنّها ليست كافية لتنظيم مثل هذه الأوراق. أنظر: **مصطفى كمال طه، وائل أنور بندق،** الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، المرجع السابق، ص346.

3- وهو ما يستدعي تغيرا في المفهوم القانوني التقليدي السائد، ويلاحظ أن هذا التغيير لن يكون قانونيا فحسب، بل .....في المقام الأول، فعلى رجال القانون أن يغيروا نظرتهم للمحرر باعتبار أن المحرر لم ولن يكون أبداً مقصورا على ما هو مكتوب على ورق وحده. **أنظر:** المرجع نفسه، الصفحة نفسها.

يؤكد على هذا المعنى المادة 5 من قانون "الأنسيترال النموذجي" التي تعرضت إلى الاعتراف القانوني برسائل البيانات، بنصها: «***لا تفقد المعلومات مفعولها القانوني أو صحتها أو قابليتها للتنفيذ لمجرد أنها في شكل رسالة بيانات***». وكذلك المادة 6 من القانون نفسه التي تنص على ما يلي: «***عندما يشترط القانون أن تكون المعلومات مكتوبة، تستوفي رسالة البيانات ذلك الشرط، إذا تيسر الإطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليه لاحقا***»[1].

ويمكن تدعيم هذا الرأي بقانون التوقيع الإلكتروني رقم 10 لسنة 2004 في مصر والذي يعترف للمحررات الإلكترونية بذات الحجية المقررة للكتابة، والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية متى استوفت شروطها المنصوص عليها على سبيل المثال في المادة الأولى من قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات حيث تنص على أن الكتابة الإلكترونية هي: «***كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى متشابهة تعطي دلالة قابلة للإدراك***»[2].

د- نظام أو ميكانيزم السفتجة الإلكترونية: يمتاز هذا النظام بالدقة مقارنة بنظام أو ميكانيزم استعمال السفتجة العادية التي تعتمد على الدعامة الورقية. فمسار أو نظام الدفع هو نفسه بين النوعين من السفتجات لكن الاختلاف يكمن في تكوين الأثر.

إن تكوين أو تقديم الكمبيالة الإلكترونية، عمل يقوم به مباشرة من طرف مؤسسة الساحب التي تستعمل نظامها الرقمي الخاص، فيكفي أن يكون لدى الساحب للكلمات السرية (codes) الرقمية ما بين البنوك، وهي عبارة عن معلومات تقدم من البنك الذي يتعامل معه الساحب [3].

1- أنظر في ذلك نص المادتين 5 و6 من قانون اليونسترال النموذجي بشأن التجارة الالكترونية الصادر عن هيئة الأمم المتحدة 1996.

2- **وائل أنور بندق،** موسوعة القانون الالكتروني وتكنولوجيا الاتصالات، المرجع السابق، ص301.

3- Ainsi est évitée la lourdeur inhérente au transfert des données écrites sur la lettre de change sur une bande magnétique, puisque le cordage sera directement effectué par le tireur .Voir : **JEANTIN Michel, PAUL Le Cannu**, Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, 5ème édition, Dalloz, Paris, 1999, p277.

وتعميم هذا الميكانيزم والإجراء الخاص بالكمبيالة الإلكترونية يقودنا بدون شك إلى انحطاط تقنية الأعمال التجارية لدعم القرض قصير الآجل، إلى جانب ذلك يقدم لنا نظرة جديدة حول ضمانات الدفع التي تعتمد أساسا على علاقة الثقة والأمان المتبادل[1] ما بين الأطرف.

هـ - خصائص السفتجة الإلكترونية: يرى اتجاه من الفقه أن السفتجة الإلكترونية تخضع لذات القواعد التي تخضع لها السفتجة التقليدية، والشيء الذي يختلف هو الخصوصية التي تمتاز بها السفتجة الإلكترونية والتي يمكننا استنتاجها فيما يلي:

- في حالة الكمبيالة الإلكترونية الورقية، جرت العادة أن تصدر على نموذج مطبوع يسمح بالإطلاع عليه بواسطة الحاسوب، وهو ما تثيره فكرة الشكلية المادية التي توجد في هذا النوع من الكمبيالة، بالإضافة إلى الشكلية القانونية.

- لكي تنشأ الكمبيالة الإلكترونية لابد من توافر البيانات الإلزامية، ولكن جرت العادة في هذا النوع على وجود بيانات أخرى، مثل اسم بنك المسحوب عليه، ورقم حسابه، واسم الفرع الذي يوجد لديه الحساب.

- تثور الصعوبة – وليست الاستحالة – في تصور قيام بعض العمليات الواردة على الكمبيالة الإلكترونية مثل التظهير والقبول، والضمان الاحتياطي، والواقع أن صعوبة ذلك لا تنفي تطبيق أحكام قانون الصرف، طالما وجدت إمكانية القيام بمثل هذه العمليات[2].

1- «Elle implique aussi une nouvelle conception des garanties de paiement reposant davantage sur des relation des confiance mutuelle que sur des garanties réelles ou mêmes personnelles ». Voir : **JEANTIN Michel, PAUL Le Cannu**, Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, Op.cit, p277.

2 - **مصطفى كمال طه، وائل أنور بندق،** الأوراق التجارية ووسائل الدفع الالكترونية،المرجع السابق، ص349.

الفرع الثاني
الشيك الإلكتروني نظير للشيك الورقي

يعتبر الشيك الوسيلة الثانية التي طورت، فلم يعرف المشرع الجزائري الشيك وإنما اكتفى بالنص على بياناته في المادة 472 من القانون التجاري الجزائري[1] ولم تذكر ما إذا أمكن إصداره إلكترونيا وإنما يظهر ذلك ضمنيا في قانون النقد والقرض والتنظيم 97-03 المتعلق بغرف المقاصة في المادة 3 فقرة2 من هذا الأخير[2].

فبعدما كان يستعمل الدعائم الورقية في المعاملات التقليدية، طورت هذه الوسيلة وأصبح اليوم يستعمل الشيك المعالج رقميا، أو ما يسمى بالشيك الإلكتروني.

فالشيك الإلكتروني يسمح بالقيام بالدفع بين طرفين، مرورا بوسيط، وطريقة الدفع هذه تختلف عن طريقة استعمال الشيك الكلاسيكي، نظرا لما تحمله من خصوصية هذه الشيكات المعالجة الكترونيا والمتداولة عبر قنوات الاتصالات. فيقوم الوسيط بخصم مبلغ الشيك من رصيد المستعمل إلى رصيد الشركة[3] ويعتبر أكثر الأوراق التجارية التي يمكن الاستفادة منها في مجال تقنية المعلومات والمعالجة الإلكترونية لها.

أولا- تعريف الشيك الإلكتروني:

يعرف الشيك الإلكتروني بأنه محرر ثلاثي الأطراف، معالج الكترونيا بشكل كلي أو جزئي، يتضمن أمراً من شخص يسمى الساحب إلى البنك المسحوب عليه، بأن يدفع مبلغا من النقود لإذن شخص ثالث يسمى المستفيد[4].

1 - أنظر المادة 472 من القانون التجاري الجزائري التي نصت على البيانات التي يجب أن يحتويها الشيك.

2 -Article 3 du règlement no 97-03 du 16 Rajab 1418 correspondant au 17 novembre1997 relatif à la chambre de compensation, jora no 17 du 25-03-1998 : « la chambre de compensation a pour mission de faciliter à ses adhérents, par compensation journalière entre eux, le règlement des soldes.
« De touts les moyens de paiement scripturaux ou électronique dont notamment des chèques… » Voir aussi : l'article 69 de l'ordonnance 2003-11 relatif a la monnaie et le crédit.

3-**SMITH Rob et SPEAKER Mark et THOMSON Mark,** Comment faire votre commerce sur internet, édition campus presse, Paris, 2000, p. 136.

4 - **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، المرجع السابق، ص351.



كما يمكن اعتبار الصك الإلكتروني (Electronic cheks) نضير للصكوك الورقية التقليدية، التي اعتدنا التعامل بها، والصك الإلكتروني هو رسالة الكترونية موثقة ومؤمنة يرسلها مصدر الصك إلى مستلم الصك (حامله)، ليعتمده ويقدمه للمصرف الذي يعمل عبر الإنترنت، ليقوم المصرف بتحويل قيمة الصك المالية إلى حساب حامل الصك. وبعد ذلك يقوم بإلغاء الصك وإعادته الكترونيا إلى متسلم الصك(حامله)، ليكون دليلا على أنه قد تم صرف الصك فعلا وانقضى التزام الدفع، ويمكن لمستلم الصك أن يتأكد الكترونيا من أنه قد تم بالفعل تحويل المبلغ لحسابه[1] وذلك بإمكانية مراقبة حركة حسابه على الخط مباشرة.

إذن تعتبر الشيكات الإلكترونية وسيلة دفع على الخط، حيث تتلاءم مع معاملات البنوك الحديثة، حيث تسعى إلى استبدال الشيك الورقي بنوع إلكتروني يستعمل فيه توقيع الكتروني حتى يتم التعرف على المستهلك على الخط[2]، وكذلك إعطائه صبغة قانونية.

ويخضع الشيك الإلكتروني لذات الأحكام التي تحكم الشيك التقليدي، كما يخضع فيما لا نص فيه لقواعد العرف المصرفي[3].

---

1 - **منير الجنبيهي،** البنوك الالكترونية، دار الفكر الجامعي، دون بلد النشر، 2006، ص49.

2- **James T. Perry et GARY P.Schneider**, E-Commerce, Editions Reynold Goulet, 2002, p508.
Le chèque virtuel s'agit purement et simplement de la transposition du mécanisme du cheque papier. Le client disposant d'un carnet de cheque virtuel et la signature manuscrite étant remplacée par une signature digitale .voir : **Dominique MOUGENOT**, Droit des obligations « la preuve», édition Larcier, 3 eme Edition, Bruxelles, 2002, p.318.

3- ومن المعلوم أن ضمانات الوفاء بالكمبيالة هي مقابل الوفاء والقبول، والتضامن والضمان الاحتياطي، ولا محل للقبول في الشيك، لأن الشيك وهو واجب الدفع لدى الإطلاع إنّما يقدم إلى المسحوب عليه للوفاء لا القبول ومن ثم تقتصر ضمانات الوفاء بالشيك على مقابل الوفاء، وهو من أهم الضمانات التي يعتمد عليها حامل الشيك.

كما يجب أن يكون مقابل الوفاء مساويا بالأقل لمبلغ الشيك، ويكون دينا بمبلغ من النقود، ويجب أن يكون مقابل الوفاء موجودا وقت إصدار الشيك، كذلك أن يكون مقابل الوفاء جائز التصرف فيه بموجب الشيك. أنظر: **مصطفى كمال طه، وائل أنور بندق،** الأوراق التجارية وسائل الدفع الالكترونية الحديثة، المرجع السابق ص350.

ثانيا- تداول الشيك الإلكتروني:

أدى استعمال الشيك الكلاسيكي على الدعائم الورقية إلى ضخامة الوسائل المستعملة لمعالجتها بين البنوك والمؤسسات المالية، ولهذا الغرض تجتمع هذه المؤسسات في مركز المقاصة المتواجد في المدن الكبرى، وذلك لانقضاء التزامات كل طرف اتجاه الآخر، وهذا النظام يعتمد على الاستعمال الهائل للورق الذي يأخذ زمنا طويلا لمعالجته.

ولهذا الغرض، وللتقليل من هذه العيوب، تم إحداث نظام تبادل صور الشيكات على الكمبيوتر[1]، كما سعت إليه فرنسا، فقد أنشأت تسعة (09) مراكز للمبادلات الخاصة بالتسجيلات الرقمية، وتم وضع نظام (CREIC) الذي يعتمد على انتقال الشيكات الكترونيا حيث يتم الوفاء بالشيك الإلكتروني في غالب الأحيان 48 ساعة بعد استلامه مـن البنك كما تمّ وضع نظام وطني للتداول الشيك الالكتروني (System National d'Echange d'Images Chèques ''SNEIC'') للتقليل من المدة التي تفصل بين الاستلام ودفع الشيك الإلكتروني، وبين المعاملات البنكية[2]، والتي من شأنها تغيير التوازنات الاقتصادية الحالية.

ذلك بتغيير التوقيع اليدوي الذي يستبدل بتوقيع رقمي أو الكتروني، وهذا النوع من نظام الدفع يستلزم وضع نظام (Logiciel) خاص بذلك ويتم التداول بمراحل يكون الفارق الزمني بينها قصير جدا ويتم وفق مراحل التي سنتناولها كالتالي:

1- المرحلة الأولى:

يصدر البنك للزبون أو المستهلك دفتر صكوك أو دفتر شيكات الكترونية بأرقام تسلسلية في الإطار المخصص له في موقع البنك التي يكون رصيده لديها، فيمكنه استعمالها بإرسالها على الخط مباشرة، أو عن طريق نظام خاص بالمتعاملين، فيكفي أن

1- **TOERING Jean Pierre et BRION François,** les moyens de payements, op.cit., p 81.

2- Par conséquent, à l'aube du III millénaire, malgré tous les efforts remarquables qui ont été conduits, le Système français d'échanges interbancaires, reste encore très marqué par l'utilisation du papier, d'énormes masses sont toujours manipulées. Voir : Ibid, p81.

يملأ الشيك على الدعامة الإلكترونية كالشيك العادي، ويتم توقيعه الكترونيا(Chiffré) أي توقيع مرقم.

واعتمادا على نظام القراءة الأوتوماتيكية للشيكات، يتم بعث أمر الدفع الإلكتروني مباشرة إلى البنك[1]، وتقوم هذه الأخيرة بدفع مبلغ الشيك كما لو أنّه شيك على دعامة ورقية.

2-المرحلة الثانية:

في هذه المرحلة يقوم البنك أو المؤسسة المالية بالتأكد من العملية المالية، حيث تعلم المستهلك على الخط دائما، وذلك بالإشارة إلى رقم الشيك وكذلك مبلغ العملية، والجدير بالذكر أنه إذا كان الشخص مالكا لرصيد اتفاقي بخصوص شبكات عادية، فإنه لا يستلزم فتح حساب جديد لاستعمال الشيكات الإلكترونية[2]. فيستفيد من خدمة الشيكات الإلكترونية اعتمادا على استعمال البنك الوسيط لشبكة العنكبوتية دون فتح حساب أخر بالضرورة.

ثالثا: نظام غرف المقاصة لتخليص الشيكات الإلكترونية :

تستلزم عمليات انتقال ودفع الشيكات الإلكترونية وضع نظام مركزي لمعالجتها وهذا ما يسمى بغرف أو مراكز المقاصة (Chambre de compensation)، وهذا النظام يقوم بتحويل مبلغ الشيك من حساب المستهلك أو الزبون المدين إلى حساب التاجر الدائن ولقد تمت معالجة حوالي 42 مليون شيك الكتروني سنة 2000 في فرنسا[3].

وظهرت العديد من المؤسسات التي تقدم خدمة الدفع بالشيكات الإلكترونية، منها مؤسسة (Chekfree corporation et Net banque) في الولايات المتحدة الأمريكية. أما في فرنسا فإن نظام حاسوب المقاصة (Ordinateur de compensation) تم اختراعه وتسييره من طرف بنك فرنسا (Banque de France) منذ 1972[4]. والغرض من هذا

1- **James T. Perry et GARY P.Schneider**, E-Commerce, op.cit., p 508.
2- Checkfree fondé en 1981 par Peter Kight, offrait un Système Automatisé de paiement mensuel et de… Checkfree cherche à devenir un fournisseur de services touchant tout type de transactions électronique pour les consommateurs et les entreprises. Voir : Ibid, p 509.
3-**James T. Perry et GARY P.Schneider**, E-Commerce, op.cit., p509.
4-**CH. Gavalda E. Michel,** Travaux dirigés de droit des Affaires- effets de commerce, Chèques carte de crédit, Editions Litec, Paris, 1994, p1999.

النظام هو تسهيل العمليات التي تستعمل فيها الأشرطة المغناطيسية التي تمثل دعامة للشيكات الإلكترونية، ولأوامر الدفع، وكذلك للكمبيالات الكلاسيكية والإلكترونية، ومنذ 1993 اعتمد على نظام آخر وهو نظام ما بين البنوك للمقاصة الإلكترونية (Système Interbancaire de télécompensation)، والذي امتد نشاطه حتى معالجة الدفع بالبطاقات البنكية[1].

1- نظام ما بين البنوك للمقاصة (Système interbancaire de compensation):

عبارة عن نظام يقوم بتسيير العمليات البنكية غير المادية الخاصة بكافة وسائل الدفع، باستثناء الشيك الكلاسيكي، وتقوم مجموعة من البنوك بتسييره إلى جانب بنك فرنسا.

لقد تم اعتماد هذا النظام في بداية التسعينات، ليحل محل حاسوب المقاصة، ليقوم بدوره بالمقاصة بين المتعاملين، والدفع الذي يتم بالوسائل الإلكترونية، وعرف هذا النظام إقبالا هائلا خاصة منذ 2002، حيث أصبح النظام الوحيد الذي يقوم بتداول وسائل الدفع فأصبح يقوم بـ 45 مليون عملية دفع ومقاصة يوميا، والتي تمثل بدورها حوالي 19 مليار أورو، وهذا التطور جاء كنتيجة للتطور التدريجي لوسائل الدفع الإلكترونية وتنحية طابعها المادي (La dématérialisation) [2].

والجدير بالذكر في هذه النقطة هو أن الجزائر وبموجب التنظيم 97-03 نظم في مادته الثالثة تسيير ومهام غرفة المقاصة ،التي تهدف أساسا إلى تسهيل العمليات المالية اليومية للمشتركين فيما بينهم بغض النظر عن الوسائل المستعملة عادية كانت أم إلكترونية يتحمل مصاريف تسييرها المشتركين فيها حسب الشروط المقررة من طرف البنك الجزائري. وتشير المادة 18 من التنظيم أنه يقصد بعملية مقاصة «***كافة العمليات التحويلية اليومية بين البنك الجزائري والأعضاء من جهة وبين الأعضاء فيما بينهم من جهة***

1- **TOERING Jean Pierre et BRION François,** les moyens de payements, op. cit, p82.

2- Le S.I.T est géré par le groupement pour un système interbancaire de télé-compensation (S.I.T), crée en 1983 par les principales banques françaises, La Poste et la Banque de France. Voir : **BOUYALA Régis,** Le monde des paiements, Édition Revue banque, 2005, p 93.

أخرى، لصالح صاحب الحساب لدى المشتركين فيها بكافة وسائل الدفع التقليدية والإلكترونية. ويتم ذلك في مقر الغرفة وبحضور ممثل لكل عضو معني بالعملية التحويلية»[1] فإذا كانت هذه العمليات يومية فهي تساير إلى حد كبير متطلبات التجارة الإلكترونية التي تسعى كافة الدول إلى تطويرها.

ومن بين أنظمة المقاصة الأكثر استعمالا في فرنسا نظام "SIT" فهو نظام دفع بالمقاصة متعدد الأطراف، الذي يعالج العمليات ما بين المشتركين على ثلاثة مراحل:

- تبادل مستمر لأوامر الدفع ما بين مراكز الإعلام الآلي والمراكز الإلكترونية البنكية مباشرة.
- مقاصة متعددة الأطراف للأوامر من طرف مركز المحاسبة.
- دفع المبالغ الصافية في نظام TBF (**T**ransfert **B**ancaire des **F**onds).

يتكون هذا النظام أساسا من معدات وبرامج (logiciels) وروابط الاتصالات، موزعة على الإقليم الفرنسي، ويمكننا التمييز:

- **المراكز (Stations):** وهي عبارة عن نقطة السماح للبنوك بالدخول إلى النظام، حيث تمثل حواسيب صغيرة (mini ordinateurs) مثبتة في مراكز الإعلام الآلي للمؤسسات المالية ومؤسسات القرض.
- **المراكز المشتركة التابعة لنظام (SIT):** لمركز التسيير ومركز النجدة. ويتم تسيير ومراقبة نظام ما بين البنوك للمقاصة (SIT) عن بعد كليا[2].

2- مبدأ عمل نظام (SIT):

يتم إشعار النظام عن طريق البنك مقدم الخدمة على النظام نفسه، حسب طبيعة الخدمة أو العملية، ويتم على شكل رسالة يعبر عنها (M1)، وكل رسالة (M1) يبعث بدوره عن طريق نظام (SIT) إلى صندوق البريد المشترك الذي توجه إليه هذه الرسالة

1- أنظر المادة 03 والمادة 18 من التنظيم 97-03 المؤرخ في 16 رجب 1418 الموافق ل 17 نوفمبر 1997 المتعلق بغرفة المقاصة الجريدة الرسمية 17 المؤرخة في 03/25/ 1998 .

2- **BOUYALA Régis,** Le monde des paiements, op.cit, p94-95.

يترتب عن إرسال الرسالة أي (M1) انقضاء الالتزام اتجاه المركز الذي بعث الرسالة الأولى، ويعبر عن هذا الانقضاء برسالة أخرى أي (M2).

فتقوم الجهة الأولى التي أرسلت الرسالة (M1) إلى نظام (SIT)، بإجراء ملخص حسابي للمبادلات، يسمى (M3) والتي تبعث بدورها إلى مركز المحاسبة، وذلك لتسوية الحسابات بين حسابات المشتركين المعنيين بالأمر[1].

من خلال ما تقدم، يمكننا تعريف نظام التحويلات المالية الإلكترونية على أنّه عبارة عن: «**عملية منح الصلاحية (Permission) لبنك ما للقيام بحركات التحويلات المالية الدائنة والمدنية، (Crédit et débit) الكترونيا، من حساب بنكي إلى حساب بنكي آخر، أي أن عملية التحويل تتم إلكترونيا عبر أجهزة الكمبيوتر والهواتف وأجهزة المودم عوضا عن استخدام الأوراق».**

وتنفـذ عـمليات التحويل المالي عن طريق دار الـمقاصة الآلـية (Automatic Clearing House (ACH))، وهي شبكة تعود ملكيتها وأحقية تشغيلها إلى البنوك المشتركة بنظام التحويلات المالية الإلكترونية، ومنذ عام 1978 أصبحت مؤسسة (EFI Corporation) تتيح للشركات والمؤسسات تحصيل تحويلاتها المالية الكترونيا عبر دار المقاصة الآلية (ACH)، وتميزت هذه الخدمة عن النظام القديم أي النظام الورقي بأنها أسرع وأنجع على معالجة مختاف خدمات التحويلات المالية [2].

1-Le principe opérationnel des échanges est le suivant :

- Une remise d'une banque émettrice, homogène par type d'opération, est éclatée » dans le réseau S I T suivant la destination, des opérations aux messages dénommée M1 ; chaque message M1 est acheminé par le S I T vers la boite aux lettres du participant récepteur.
- Le dépôt du message M1 dans la boite aux lettres provoque l'envoi d'un acquittement, dénommé : Message M2, vers la station émettrice.
- Cette dernière crée un résumé comptable de l'échange dénommé message M3, qui est envoyé au centre comptable pour mise à jour des comptes SIT des participations concernées. Voir : **BOUYALA Régis,** Le monde des paiements, op.cit, p 95.

2 - **منير الجنبيهي،** البنوك الالكترونية، المرجع السابق، ص37.

المطلب الثاني
وسائل الدفع الإلكترونية الحديثة

لم يتوقف التطور التكنولوجي في مجال المعلوماتية والاتصال في التجارة الإلكترونية، عند حد المعالجة الإلكترونية لوسائل الدفع الكلاسيكية، بل تم اختراع ووضع أدوات وليدة التجارة الإلكترونية نفسها، خاصة وأن للعقد الإلكتروني طبيعة غير مادية، يلتزم المشتري بالوفاء بالتزاماته المتمثلة بدفع الثمن، فلا بد أن يكون الثمن الكترونيا[(1)].

وتعتبر من أهم الخدمات المصرفية الحديثة التي استحدثتها المصارف التجارية في الولايات المتحدة الأمريكية في سنوات الستينات، وتتلخص هذه الخدمة في منح الأفراد بطاقات من البلاستيك تحتوي على معلومات المتعامل ورقم حسابه على شفرة أو شريط مغناطيسي، وبموجب هذه البطاقة يستطيع المتعامل أن يستفيد بعديد من خدمات في المجالات التجارية بوساطة المصارف وقبولها منح الائتمان لحامل البطاقة [(2)].

ولقد حظيت هذه الوسائل باهتمام خاص من طرف المتعاملين مما جعلها مركز مناقشة ودراسة لتنظيم التعامل بها وتأطيرها من قبل هؤلاء المتعامين في مختلف الدول[(3)]، وتعد من الوسائل الأكثر استعمالا، التي تعتبر ثورة في ضوء التجارة الإلكترونية والبطاقات البنكية المختلفة التي سيتم دراستها (فرع أول)، وهي وسيلة تترتب عنها التزامات للأطراف المشتركة في علاقتها القانونية والتي تستوجب وضع نظام قانوني لها ينظمها تنظيما محكما(فرع ثاني).

---

1 - **جلال عايد الشورة**، وسائل الدفع الالكتروني، دار الثقافة للنشر والتوزيع، مصر، 2008، ص19.

2- **زياد سليم رمضان، محفوظ أحمد جورة**، الاتجاهات المعاصرة في إدارة البنوك، ط2، دار وائل للنشر والتوزيع، 2003، ص18.

3 - Commission européenne, DG concurrence, intérim report 1 : payement card, Article 17 régulation 1/2003 ou E- Banking, 12 Avril 2006, p2. Publié sur :www.wikipedia.org/wiki/cartdepaiement.

الفرع الأول

البطاقات البنكية

لم تنشأ بطاقات الوفاء والائتمان نشأة مصرفية كما قد يتصور البعض، فقد نشأت في الولايات المتحدة الأمريكية في عام 1914 على يد شركات البترول، التي أصدرت هذه البطاقات لعملائها لشراء ما يحتاجون له من منافذ التوزيع التابعة لها، وتسوية الحساب في نهاية كل مدة زمنية، ثم طورت هذه البطاقات واستخدمتها المحلات التجارية والفنادق.

وقد اختلفت التسميات التي أعطاها الفقه لهذه البطاقات، فيسميها البعض البطاقات البلاستيكية، والبعض الأخر يسميها البطاقات الدائنة، والبعض يسميها بطاقات الوفاء أو البطاقات البنكية أو بطاقات الائتمان...الخ [1].

وحسب تقديرنا فإن تسمية البطاقات البنكية، هي التسمية الأنسب، وذلك لحصرها لكافة البطاقات باختلاف وظائفها من جانب، وكذلك للدور الفعال الذي تقوم به البنوك في العملية المصرفية التي تستعمل فيها هذه البطاقات والتي يلعب الائتمان أساس العلاقة التعاقدية لحاجتها إلى بنك أو مؤسسة مالية كوسيط في العملية النقدية، فمن المنطقي تسميتها البطاقات البنكية التي تحمل في طياتها كافة هذه البطاقات.

وما يعبر عن قوة هذا النظام، هو أن حامل البطاقة هو الوحيد الذي يكون على علم بكافة المعلومات الخاصة بالعملية، فالبائع لا يكون على علم بالمعلومات البنكية الخاصة بالمشتري، كما أن البنك لا يكون على علم بكافة جزئيات العملية. [2]

أولا-تعريف البطاقات البنكية:

عرفت المادة 543 مكرر23 تجاري جزائري بطاقة الدفع بنصها «***تعتبر بطاقة الدفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل الأموال***»[3].

---

1 - **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، المرجع السابق ص303.

2 - **WERY Etienne**, Facture , Monnaie, Litec, op.cit., p 57.

3- راجع: المادة 543 مكرر23 من القانون التجاري الجزائري.

كما اهتم الفقه بتعريف البطاقات البنكية، فقدم المجمع الفقهي لمنظمة المؤتمر الإسلامي في دورته السابعة بجدة عام 1993، تعريفا حيث أكد على أنّها: «***مستند يعطيه مصدره لشخص معين بناء على عقد بينهما يمكنه من شراء السلع والخدمات ممن يعتمد المستند، دون دفع الثمن حالا لتضمينه التزام المصدر بالدفع، ومنها ما يمكن سحب النقود من المصارف***»[1].

كما نلاحظ أن بعض الفقهاء قد عرفوا بطاقات الائتمان « **بأنّها بطاقة بلاستكية أو ورقية مصنوعة من مادة يصعب العبث بها، تصدرها جهة معينة، بنك أو شركة استثمار** » . كما يسمي البعض بطاقات الدفع بمحفظة النقود الإلكترونية التي تعد تطبيقا عمليا لفكرة الدفع المسبق للوحدات الإلكترونية، والتي تسمح بتخزين مسبق (In advance) للقيمة الشرائية، معبراً عنها بوحدات وعملات الكترونية يتم استخدامها بعد ذلك في عملية الدفع.

ويتم شحن هذه المحفظة من خلال ماكينات الشحن العادية الموجودة في أماكن عديدة، أو من خلال أجهزة التلفون مخصصة لذلك في مقابل حساب مفتوح لدى الجهة المصدرة، والتي قدمت خدمة الشحن عن طريق التليفون، أو في مقابل مبالغ تدفع في مقر البنك أو المؤسسة المالية المصدرة للبطاقة[2].

ثانيا-أنواع البطاقات البنكية:

تجدر الإشارة إلى أن السوق المالية بصفة عامة توفر العديد من أنواع الكروت البنكية، فنجد منها ما يلي :

- بطاقة الصرف البنكي، بطاقة تكون فيها مدة الائتمان شهرا من تاريخ السحب.

---

1 - كما عرف البعض بطاقة الائتمان بأنها: "بطاقة تصدر بوساطة مؤسسة مالية باسم أحد الأشخاص، وتقوم تلك البطاقة بوظيفتي... والائتمان، أي أن حاملها يملك إمكانية تتبع سداد المبالغ التي استخدمها في الاعتماد المفتوح من جانب مصدر البطاقة". أنظر في هذا الموضوع: **جلال عايد الشورى،** وسائل الدفع الإلكترونية، المرجع السابق، ص18.

2- **شريف محمد غنام،** محفظة النقود الالكترونية رؤية مستقبلية، دار الجامعة الجديدة للنشر، مصر، 2007 ص43.

- بطاقة الدفع التي تعتمد على وجود أرصدة فعلية للعملاء لدى البنك،حيث يتم تحويل ذلك المقابل من حساب العميل إلى حساب التاجر.
- بطاقة الشيكات وتصدرها البنوك لحاملي الشيكات ، وبمقتضى هذه البطاقة يضمن الوفاء في حدود معينة بقيمة الشيك الذي يصدره حاملها.وعند سحب الشيك لأحد التجار يتعين على حاملها إبراز البطاقة وتدوين رقمها على ظهر الشيك.
- بطاقة الانترنت والتي أصدرتها ماستر كارد وفيزا كارد، عبارة عن بطاقة ائتمان خاصة بالتسويق عبر الشبكة العنكبوتية العالمية مباشرة.
- بطاقة الائتمان والتي تمكن حاملها من شراء سلع وخدمات باستخدام هذه البطاقة حيث يتحصل التاجر على الثمن من البنك الذي يتولى تسويق البطاقة ثم يقوم البنك بعد ذلك بمطالبة العميل بالسداد.
- البطاقة الذكية، عبارة عن كمبيوتر متنقل تمتاز هذه البطاقة بحماية كبيرة ضد التزوير أو سوء الاستخدام، وتحتوي على كافة البيانات الخاصة بحاملها مثل الاسم، العنوان، المصرف...الخ[1].

1- تمييز محفظة النقود الإلكترونية عن غيرها من البطاقات:

إن قيام محفظة النقود الإلكترونية على فكرة الدفع المسبق، جعلها تتميز عن غيرها من الكروت البنكية من ناحيتين:

- فالكروت العادية تقوم على أساس فكرة الدفع اللاحق التي لا تجعل الدفع بهذه الكروت نهائيا إلاّ بعد موافقة البنك، ولهذا السبب يشك البعض في مدى اعتبار هذه الكروت وسيلة من وسائل الدفع، ويرون أنّها تعد وسيلة ائتمان فقط، على أساس أنّها لا يترتب عنها دفع حال وفوري، أما الدفع بمحفظة النقود الإلكترونية، فإنّه

1- **محمد أمين الرومي،** التعاقد الإلكتروني عبر الأنترنت، دار المطبوعات الجامعية، الطبعة الأولي، الإسكندرية 2004، ص131-137.

يعد نهائيا منذ وصول الوحدات إلى الكارت الخاص بمحفظة التاجر، وبالتالي يترتب عنها استخدام حال يبرئ العميل من دينه[1].

- إلى جانب ذلك فالدفع لا يكون مباشرا إذا تم بطريق الكروت العادية، فالكارت لا يحمل في ذاته نقودا يتم السداد بها، وما هو إلا وسيلة لربط العميل بحسابه البنكي حيث يتم السداد من الحساب مباشرة، أي هناك تدخل طرف ثالث وهو البنك.

والأمر على خلاف ذلك بالنسبة للدفع عن طريق محفظة النقود الإلكترونية التي تحتوي بذاتها على أموال في صورة وحدات الكترونية، التي تعبر عن قيم مالية تستخدم مباشرة في السداد، فلا تحتاج سوى إلى طرفين هما المستهلك والتاجر، أما الطرف الثالث وهو مصدر هذه الوحدات الذي يقتصر دوره على منح المستهلك هذه الوحدات من البداية وقبل عملية الشراء[2].

2- محفظة النقود الخيالية (Le porte monnaie virtuel):

على خلاف الصورة الأولى المتمثلة في محفظة النقود الإلكترونية، فمحفظة النقود الخيالية لا تستلزم دعامة مادية، فيتمثل عـادة فـي برمجيات (Logiciel) يحمل على القـرص المضغوط (Le disque dur) لكمبيوتر المشتري، هذه الخاصية تحمل في طياتها مجالات ضعف من بينها خطر فقدان القيم النقدية المتواجدة فيه في حالة التدمير المادي للجهاز أو للقرص.

ومن بين الأنظمة المطبقة في فرنسا نظام (Beenz) الذي يستعمل تقنيات جد مطورة لاستبدال هذه القيم المعبئة مقابل سلع وخدمات و(Europocket)، وهو نظام صناديق التوفير ترتكز على شراء كروت مدفوعة مسبقا، أما على المستوى الدولي يمكننا ذكر (Splashplastic, Odyssée) و(LUK Smart)[3] يذكر فيها اسم العميل الصادرة لصالحه ورقم حسابه، حيث يملك الحامل تقديم تلك البطاقة للتاجر لتسديد ثمن مشترياته

1- **شريف محمد غنام،** محفظة النقود الإلكترونية، رؤية مستقبلية، المرجع السابق، ص44.

2 - **المرجع نفسه،** ص 45.

3 - **WERY Etienne**, Facture , Monnaie, Litec, op.cit., p 135.

حيث يقوم التاجر بتحصيل تلك القيمة من الجهة المصدرة التي تقوم بدورها باستفاء تلك المبالغ من الحامل[1].

ثالثا: المواصفات التي يجب أن توفر في البطاقات البنكية:

يمكن التمييز بين المواصفات المادية الشكلية والفنية:

1- المواصفات المادية:

تصنع البطاقات من مادة بلاستكية وهي مادة «**كلوريد الفينيل**» غير المرن بمساحة حوالي 5×8 سنتم، مسجل على وجهيها بيانات أساسية، كما تحتوي على شريط مستطيل ممغنط يتم تكوينه (Enciding)، أي كتابة بيانات البطاقة على الشريط الممغنط بما يسمح بالتعرف على البطاقة عند استخدام الآلات الإلكترونية. كما قد يحتوي على دائرة إلكترونية، وهذا بالنسبة للبطاقة الذكية (Smart Card)، والبطاقة الرقائقية (Chip Card)[2].

تقدم ماديا بمقياس المعايير ISO 2894 طولها 86 مم وعرضها 45 مم، محملة بذاكرة (Microprocesseur) أو شفرة الكترونية أو شريط مغناطيسي، وهي نقطة تلاقي ما بين الدعائم الورقية والتكنولوجيا الرقمية، تحمل معلومات كتابية ظاهرة جدا (embossé)، وتوقيع يدوي، وتعتبر شعاع المعلومات المرقمة على الشريط المغناطيسي والشفرة الإلكترونية[3].

2- المواصفات الشكلية:

يجب أن يتوافر في البطاقات بعض المواصفات الشكلية، حيث يصعب تقليدها وأيضا لسهولة التعرف عليها مثل العلامات المميزة للمنظمات العالمية التي لها حق

---

1 - **جلال عايد الشورى**، وسائل الدفع الإلكترونية، المرجع السابق، ص22.

2- **نادر شعبان، إبراهيم السواح**، النقود البلاستكية وأثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، الدار الجامعية، مصر، 2006، ص27.

3 - La carte est le point de contacte de la civilisation du papier et de celle de l'informatique, elle porte en caractères apparents, des écrits embossés et une signature manuscrite, elle est surtout le vecteur d'informations numérisées sur piste magnétique et puce électronique. Voir : **PIEDELIEVRE Stéphane**, Instrument de crédit et paiement, Edition Dalloz, 3eme Édition, Paris, 2003, p 254.

الإصدار والترخيص لإصدار هذه البطاقات، ويكون دائما مقسم إلى جزئيين هما اسم وشعار المنظمة.

3- المواصفات الفنية:

وهي مثل رقم البطاقة، وتتكون من أربع مجموعات من الأرقام، ويجب أن تكون هذه الأرقام مطبوعة بطريقة بارزة، أن يوضع على البطاقة تاريخ انتهاء الصلاحية وبحروف بارزة، وأيضا توقيع حامل البطاقة، كما يجب أن يوضع اسم حامل البطاقة بطريقة بارزة. [1] كما يمكن للبنك وضع معلومات إضافية بعد موافقة المنظمات العالمية مثل صورة ملائمة الأبعاد لحامل البطاقة.

رابعا: أطراف التعامل بالبطاقات البنكية:

يشترك في التعامل بتقنيات البطاقات البنكية العديد من الأطراف التعامل حيث تنشأ بين كل طرفين منها علاقة تعاقدية ثنائية ، وتتمثل هذه الأطراف في:

1- المنظمة العالمية (المركز العالمي للبطاقة):

هي التي لها حق منح الترخيص للبنوك لإصدار البطاقات، وتقوم بدور الوسيط بين البنوك الأعضاء المتعاملة في مجال البطاقات، وإعطاء التفويضات على تنفيذ أو عدم تنفيذ العمليات التي تستخدم فيها البطاقات. كما تقوم بدور التسوية بين البنوك الأعضاء وذلك من خلال حساب التسوية الذي يفتحه كل بنك من البنوك الأعضاء فيها، ويكون تحت تصرف المنظمة، وإزالة أي خلاف بين البنوك الأعضاء. ومن الأمثلة على هذه المنظمات مؤسسة "**الفيزا العالمية**" ومنظمة "**ماستركارد العالمية**"[2].

وتملك أيضا صلاحيات في عملية حل النزاعات والخلافات الناشئة بين أطراف العلاقة القانونية، فيكون دورها في هذه الحالة دور المحكم، ويتم ذلك مقابل عمولة تتراوح عادة ما بين 1 إلى 4 % من قيمة العملية التي يدفعها التاجر، إضافة إلى اشتراك سنوي

1- **نادر شعبان، إبراهيم السواح،** النقود البلاستكية وأثر المعاملات الالكترونية، المرجع السابق، ص28.

2- المرجع نفسه، ص29.

في معظم الحالات يدفعها المستخدم (حامل البطاقة)[1]. ويحكم هذه البطاقات من الناحية القانونية وينظم العلاقات الناشئة عنها القانون الوطني الذي نظمت ونشأت في ظله، إذا كان هناك قانون ينظم هذه العمليات أو الرجوع إلى القواعد العامة في هذا المجال في حالة دم وجود قانون داخلي ينظم مثل هذه العمليات.

2- مصدر البطاقة (Issuer Bank):

هو البنك أو المؤسسة المالية التي لها أدوار عدة منها: التعاقد مع المركز العالمي للبطاقات من أجل حصولها على ترخيص يسمح لها بإصدار البطاقات من خلال دخولها في عضوية إصدار الطاقات، والتعاقد مع التجار المحليين من أجل قبول استخدام هذه البطاقات من طرف عملائها لتسوية عملياتهم من شراء أو تقديم خدمات معينة. بالإضافة إلى التعاقد مع عملائهم للتعامل بمثل هذه البطاقات في دفع ما يستحق عليهم للتاجر مقدم السلعة أو الخدمة، وحصول التاجر على عمولة مقابل ما يقدمه إلى عملائه باستخدام هذه البطاقة[2]. كما تقوم الجهة المصدرة بمتابعة حسابات حملة البطاقات، وإصدار كشف حساب البطاقة لهم، والذي يحتوي على كافة العمليات التي قاموا بتنفيذها، باستخدام البطاقة، ويلتزم بالرد على استفسارات حملة البطاقة، ومتابعة شكواهم واعتراضاتهم على العمليات المدرجة بكشوف حساب بطاقاتهم[3].

3- التاجر قابل للتعامل بالبطاقات البنكية:

هو الذي يقبل التعامل بالبطاقة مع العميل، بناء على اتفاق مسبق بينه وبين مصدر البطاقة، ويطلق هذا الوصف على الشركات أو المؤسسات صاحبة السلع ومحلات البيع

1- توجد منظمة (Visa Card) في الولايات المتحدة الأمريكية في ولاية كاليفورنيا، بمنطقة سان فرانسيسكـو وهي تقسم العالم كله إلى عدة مناطق وهي: كندا، أوروبا، أسيا، أمريكا اللاتينية، إفريقيا والشرق الأوسط والولايات المتحدة الأمريكية. وأهم إصدارتها البطاقة الذهبية (Golden card)، بطاقات رجال الأعمال (Busines card)، والبطاقات العادية (Classic card). أنظر: **جلال عايد الشورة**، وسائل الدفع الالكتروني المرجع السابق، ص36. فالقانون الفرنسي توسع في تعريف البنوك واندرجت عمليات إصدار البطاقات ضمن عمليات البنوك الخاضعة لإشراف السلطات النقدية للدولة، ولكن يظل دور هذه البطاقات بعيدا عن إشراف ورقابة هذه السلطة النقدية.

2- المرجع نفسه، ص37.

3- **نادر شعبان، إبراهيم السواح**، النقود البلاستكية وأثر المعاملات الالكترونية، المرجع السابق، ص29.

ومراكز تقديم الخدمات للجمهور بشكل عام، ويبرم اتفاقا مع مصدر البطاقة لقبول البيع بالبطاقة، ومن ثم يرجع إلى مصدر البطاقة للحصول على ثمن هذه السلعة[1].

4- حامل البطاقة (Card Holder):

هو الشخص المصرح له باستخدام البطاقة المصدرة له من أحد البنوك، وتكون البطاقة مطبوعة باسمه وموقعة بتوقيعه، ولديه الرقم السري الخاص بها، ويلتزم حامل البطاقة بشروط وأحكام البنك المصدر للبطاقة[2]. ويكون ذلك بناء على طلب تم تقديمه للمصدر ووافق على منحه إياها لتمكينه من الشراء بواسطته أو الحصول على الخدمات التي يرغب فيها، كما يمكنه السحب النقدي من الصراف الآلي باستخدام البطاقة الممنوحة من طرف مصدر البطاقة.

ويدفع حامل البطاقة للمصدر المستحقات المترتبة عليه جراء استخدام هذه البطاقة وقد يتطلب الأمر فرض البنك أو المؤسسة المالية لإجراءات خاصة. وقد يستفيد الحامل من امتيازات خاصة [3].

ويظهر ذلك من خلال تجمعات مصدري بطاقات الدفع كما حدث باتخاذ "مجمع البطاقات الزرقاء" من جهة، و"ماستركارد" و"أوروباي" من جهة أخرى. وقاموا بإنشاء تجمع البطاقات البنكية (Groupement des Cartes Bancaires). فإلى جانب الدفع

1- **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، المرجع السابق، ص357.

وهو كل المحلات والفنادق والشركات التي تقبل البطاقات كوسيلة دفع للسلع والخدمات المقدمة من خلالها، والذي بدوره يتعاقد مع أحد البنوك لتحصيل قيم الإيصالات المحررة من حملة البطاقة. أنظر: **نادر شعبان، إبراهيم السواح**، النقود البلاستكية وأثر المعاملات الالكترونية، المرجع السابق، ص30.

2- **نادر شعبان، إبراهيم السواح**، النقود البلاستكية وأثر المعاملات الالكترونية، المرجع السابق، ص29.

3- إن إصدار البنك أو المؤسسة البطاقة للعميل يجعله مسؤولا اتجاه التجار عن تسديد قيمة المسحوبات والمشتريات التي استخدمت بها هذه البطاقة، مما يجعل البنك أو المؤسسة المالية حريصة على التأكد من ملاءة العميل المالية، وقدرته على السداد، إضافة إلى تمتعه بسجل وتاريخ خال من المشاكل البنكية. أنظر: **جلال عايد الشورى**، وسائل الدفع الإلكترونية، المرجع السابق، ص38.

بالبطاقات كافة السلع والخدمات التي يتم اقتناؤها في فرنسا، تستعمل هذه العملية في الخارج خاصة وأن التاجر على علم بأن مبلغ السلع مضمون[1].

الفرع الثاني

العلاقة الثلاثية الناتجة عن استعمال البطاقات البنكية

تعتبر البطاقات البنكية من الوسائل الحديثة التي تستعمل تقنية الدفع الإلكتروني، وتتميز بشيء من التعقيد حتى تتم انقضاء التزامات الأطراف الثلاثة، كل منها اتجاه الطرف الآخر، بين كل من حامل البطاقة والبائع والبنك، وبالتالي تتم هذه العمليات بعلاقات تعاقدية بين كل منهما، مما يستدعي دراسة هذه العلاقة كالآتي:

أولا: العلاقة بين البنك مصدر البطاقة والعميل أو الحامل:

يبرم العقد بين مصدر البطاقة والعميل كغيره من العقود التي تحتاج إلى إيجاب وقبول، ويتم هذا العقد كتابة[2]، فإن مسؤولية طرفي العقد تكون نتيجة ما تم الاتفاق عليه والمتمثلة في كيفية استخدام هذه البطاقة، ومدة صلاحيتها للاستخدام، والحد الأقصى المسموح لحاملها بالشراء في حدوده، والطريقة التي يتم التسديد بها، ونسبة الفائدة التي يحصل عليها مصدر البطاقة[3].

---

1 - Fonction accréditive de la carte qui inspire davantage confiance que le chèque. Voir : **PEROCHON François**, Entreprise en difficulté instrument de droit et de paiement, L.G.D.J, 4ème édition, Paris, p 678.

2 - **جلال عايد الشورى،** وسائل الدفع الإلكترونية، المرجع السابق، ص39.
والكتابة هنا ليست شرطا للانعقاد بل للإثبات، وهذا ما أشارت إليه توصية 30 جويلية لسنة 1997، الصادرة عن الاتحاد الأوروبي التي نصت على:
« **Les clauses du contrat doivent être présentées en termes simples et aisément compréhensibles ».**

3 - لا يعتبر هذا العقد من عقود البيع بالتقسيط، بل هو عقد ذو طبيعة خاصة به، تتمثل في منح العميل أجل للوفاء بما يستحق عليه من جراء هذه العمليات، ويعتبر قرضا شخصيا مسحوبا على مصدر البطاقة باعتماد مخصص.
أنظر: **جلال عايد الشورى،** المرجع نفسه، ص 38.

ومن بين شروط تكوين العقد أيضا، أن يكون حامل البطاقة ذو أهلية للقيام بأعمال أو أفعال ، وذلك لأن الحصول على بطاقة بنكية لا يعتبر فعل قانوني ويمكن للحامل أن لا يقوم بالعمليات البنكية عن طريق البطاقة سوى مع أشخاص ذوي أهلية قانونية[1].

كما يمكن إصدار العديد من بطاقات الدفع لحساب بنكي واحد، وهذا ممكن في حالة الحساب الجماعي، أو الحساب الذي يكون صاحبه شخص معنوي، أو في حالة ما إذا كان صاحب الحساب يرغب في تقديم البطاقات للمستخدمين التابعين له، لتسهيل عملهم مثلا[2]. وتنص العقود في هذه الحالة على أن صاحب الحساب وحاملي البطاقات متضامنين فيما يخص العمليات التي تتم بالبطاقات البنكية من هذا النوع.

ورغم عدم وجود نصوص قانونية فيما يخص تقديم البطاقات، فالبنك لا يلتزم بتقديم بطاقات بنكية لكل زبائنه الذين يقومون بطلب ذلك، وإنما كل ذلك يرتكز على الأمان. وبالتالي فإن ملكية البطاقة تكون للبنك المصدر لها، ويمكنه في كل وقت سحبها من حاملها أو رفض تجديدها، وهذا حسب بنود العقد، ويشترط العقد أو الاتفاقية أن يكون الرفض مسبب، يمكننا أن نلتمس نوعا من التعسف في استعمال هذا الحق [3].

وتنص الاتفاقات النموذجية على أن عدم احترام هذه الالتزامات يؤدي إلى قيام حق مصدر البطاقة في استرجاع البطاقة، وإلزام الحامل بإرجاعها له[4].

وفي حالة ضياع البطاقة يلزم مصدر البطاقة العميل القيام بالإبلاغ مباشرة بالطريقة التي تم الاتفاق عليها في العقد، وإلا تحمل حاملها نتيجة ذلك، فيعتبر حاملها

1- La détention d'une carte n'est pas un acte juridique et que le porteur pouvait n'effectuer avec la carte que les opérations qu'il a la capacité d'effectuer, 'ex : actes de la vie courante ..) mais pratiquement opportune en raison du risque élevé que courrait l'incapable ou le tiers. Voir : **PEROCHON François**, Entreprise en difficulté instrument de droit et de paiement, op.cit., p 680.

2- Les contrats prévoient en ce cas le titulaire du compte et celui de la carte sont solidairement tenus du paiement des opérations effectuées avec la carte. Voir : Ibid, p681.

3-Ibid, p 681.

4-**JEANTIN Michel, PAUL Le Cannu**, Droit commercial: instruments de paiement et de Crédit, entreprise en difficulté, op.cit., p 127.

وتجدر الإشارة في نفس السياق إلى أن البطاقة تصدر من مصدرها إلى شخص معين بالذات، ولا يملك هذا الأخير حق التنازل عنها لغيره، لأن البطاقة تحمل توقيعه، وهو وحده الذي يملك حق التوقيع واستخدام هذه البطاقة في عمليات الشراء أو الصول على خدمة معنية بطلبها. أنظر: **جلال عايد الشورى،** وسائل الدفع الإلكترونية، المرجع السابق، ص40.

مسؤولا عن البطاقة حتى لحظة تبليغ المصدر بالسرقة أو الضياع[1]. ومن الممكن أن يكون التبليغ بواسطة الهاتف لتحقيق السرعة في إخطار مصدر البطاقة، ثم يلحقه تبليغ كتابي، وهذا ما جرى عليه العرف، إلاّ إذا تم الاتفاق على طريقة معينة أخرى في العقد، كما يلتزم ببيان طريقة فقدانها.

يقوم صاحب السلعة أو الخدمة من الزبون التوقيع على الفاتورة النموذجية المتضمنة ما طلبه الزبون، والمعدة خصيصا والمدون فيها ما طلبه الزبون [2]، وبمجرد توقيع حامل البطاقة على هذه الفواتير يعد مصدرها ملتزما بالوفاء بقيمة هذه الفواتير.

يعد ما ينتج من أثر قانوني عن توقيع حامل البطاقة على الفواتير اعترافا وإقرارا بما ورد في هذه الفاتورة، وبذلك تكون ذمته المالية مشغولة بدين التاجر أو مقدم الخدمة ولا تبرأ ذمة موقع الفاتورة مما ترصد له جراء حصوله على السلعة أو الخدمة، إلاّ بالوفاء الفعلي من مصدر البطاقة للتاجر، وبذلك تبرأ ذمة موقع الفواتير تجاه التاجـر وتبقى ذمته مشغولة لمصدر البطاقة حتى يستوفي مصدر البطاقة ما تم دفعه للتاجر حامل البطاقة[3].

1- حقوق العميل حامل البطاقة:

يرتب العقد بين مصدر البطاقات البنكية وحاملها حقوق للحامل أو العميل وتتمثل فيما يلي:

- يملك حامل البطاقة خلال فترة زمنية معينة غالبا تكون 30 يوما من تاريخ تبليغ أو إصدار كشف الاعتراض على أية عملية، كما يحق له الحصول على كشف عن حسابه.

1- كما يحتفظ مصدر البطاقة خلال فترة من الزمن بحق تقديم حامل البطاقة للإبلاغ لتمكنهم من اتخاذ بعض الإجراءات المطلوبة، مثل تبليغ التجار عن عدم قبول هذه البطاقة المفقودة. أنظر: **جلال عايد الشورى،** وسائل الدفع الإلكترونية، المرجع السابق، ص43.

2- المرجع نفسه، ص40.

3- نفسه، ص40-41.

كما يجب على العميل طالب البطاقة أن يوقع على طلب الحصول على البطاقة التي تحتوي معلومات متعلقة به، مثل حالته الشخصية وطبيعة عمله، والحالة المالية له[1].

يعتبر عقد الحامل عقد محدد المدة (سنة أو سنتين) أي مدة صلاحية البطاقة والمذكورة على البطاقة نفسها، وهي قابلة للتجديد [2].

كما يحتفظ مصدر البطاقة بحقه في تعديل بنود العقد متى رأى ذلك ضروريا فيتم إخطار حامل البطاقة ويمنح له ميعاد شهر عادة لإرجاع البطاقة وإنهاء سريان العقد.

2- التزامات حامل البطاقة:

يلتزم حامل البطاقة بالتوقيع الإلزامي على البطاقة، وكذا الاستعمال اللائق والقانوني للبطاقة، كما يلتزم كذلك في حالة النزاعات التي تنشب عند ضياع البطاقة أو سرقتها منه، بذل كل جهده لتبليغ مصدر البطاقة في أسرع الآجال لأنّها ملك لهذا الأخير وممنوحة للحامل إلاّ على شكل تسلفة للاستعمال، الشيء الذي يجعله في حالة عدم الاسترجاع أو عدم التبليغ في الوقت المناسب إلى متابعة للتعسف في الثقة[3].

---

1 - وقد يحتفظ مصدر البطاقة بحقه في رفض أو قبول الطلب، كشرط في العقد، فإن وجد مثل هذا الشرط فله ذلك، ويكون بعد توقيع الطلب من طالب البطاقة، فيرسل موافقته إلى العميل إن وافق، وإذا ورد مثل هذا الشرط فهو صحيح، لأن العقد شريعة المتعاقدين، وهو يقوم على اعتبار شخصي وتجدر الإشارة إلى أنّه في حالة حضور العميل يقوم كل من رئيس ومراقب قسم الحسابات الجارية بتسليمه البطاقة الخاصة به بعد قيامه بالتوقيع على ظهرها بنفس التوقيع الموجود بالفرع، وكذلك بتسليم ظرف مغلق به الرسم السري الخاص به على أن يقوم بالتوقيع على إيصال الاستلام. أنظر: **جلال عايد الشورى،** وسائل الدفع الإلكترونية، المرجع السابق، ص39.

2- «… Tacite reconduction sauf dénonciation par le porteur ou par le titulaire du compte dans les délais prévus exprès de deux mois à la charge du porteurs, alors qu'en cours de contrat le titulaire droit de restitution comme l'émetteur droit de retrait peuvent y mettre fin à tout moment discrétionnairement la clôture du compte y met fin automatiquement et oblige le porteur de restituer la carte, voir : **PEROCHON François**, Entreprise en difficulté instrument de droit et de paiement, op.cit., p 683".

3 - **JEANTIN Michel,** Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, op.cit., p 126.

كما تنص معظم العقود النموذجية في حالة البطاقات المقدمة للمؤسسات إلى التضامن في تحمل الالتزامات بين صاحب الحساب البنكي وحامل البطاقة عند استعمالها وضرورة الحفاظ عليها[1].

إن التزام الحامل بالتوقيع على البطاقة غرضه التقليل من مخاطر استعمال البطاقة البنكية، كاستعمال البطاقة المسروقة والاستعمال الخاطئ للبطاقة، فيلتزم أساسا بالاستعمال اللائق للبطاقة وفقا لما تنص عليه العقود النموذجية، بالتالي لا يجب استعمال البطاقة إلا للغرض الذي صدرت من أجله، من طرف مصدر البطاقة، وغالبا ما يكون في نهاية كل شهر، والإشارة إلى الحركات التي أجريت عليه لبيان ما إذا كانت هناك أية اعتراضات على الحساب، فإن وجد العميل ما يعترض عليه يقوم هذا الاعتراض لمصدر البطاقة[2].

3- التزامات مصدر البطاقة:

يرتب العقد بين المؤسسة مصدرة البطاقة وطالب الحصول عليها، التزامات على مصدر البطاقة كذلك فهو عقد ملزم للجانبين.

أ- الالتزامات اتجاه حامل البطاقة: يلتزم مصدر البطاقة بإبلاغ الطالب للحضور لاستلام بطاقته البنكية، والرقم السري الخاص به، خلال الفترة المتفق عليها من تاريخ إخطاره، وهي في العادة 40 يوما، يعد بها كشف يعرض على السيد مدير الفرع، لاتخاذ ما يراه مناسبا كأن يستدعي العميل أو ينتظر عودته من الخارج، أو اتخاذ قرار بإعدامها[3].

---

1 - **JEANTIN Michel,** Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, op.cit., p 126.

2 - وفي هذه الحالة يقوم مصدر البطاقة بإخطار الإدارة العامة للبطاقة بصورة عن الاعتراض بعملية (change Back)، أي الفحص والاستعلام عما تم الاعتراض عليه، فإذا ثبت عكس ما يدعيه حامل البطاقة يتحمل المعترض كافة المصاريف. أنظر: **جلال عايد الشورى،** وسائل الدفع الإلكترونية، المرجع السابق، ص42.

3 - **نادر شعبان، إبراهيم السواح،** النقود البلاستكية وأثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، المرجع السابق، ص 40.

يلتزم مصدر البطاقة القيام بعملية فرز الأشخاص الذين بإمكانهم الحصول على البطاقة، ولم ينص أي نص تشريعي على هذا الالتزام، وإنّما مستوف من قرار محكمة النقض الفرنسية، على أنه لا يمكن لعديم الأهلية الحصول على بطاقة بنكية دون مساعدة الولي الشرعي أو القانوني له، وهذا القرار يؤكد على التزام مصدر البطاقة التأكد من أهلية الشخص الذي يتعاقد معه، ومخاطر إصدار بطاقة بنكية لعديم الأهلية يتحملها البنك المصدر، إذا خالف قواعد الأمان والضمان التي تستوجبها هذه العملية والتي يخضع لها[1].

كما يلتزم مصدر البطاقة أساسا بالتعهد بالدفع باسم ولحساب الحامل أو العميل مبالغ الاقتناءات من السلع والخدمات التي قام بها الحامل باستعمال بطاقة الدفع، بالاعتماد على الفواتير التي يتلقاها من طرف التاجر أو مقدم الخدمة، أو من طرف البنك الذي يتعامل معه التاجر.

فيدفع بكونه ضامن(Mandataire) لحامل البطاقة، فيدفع للتاجر مشتريات حامل البطاقة، إذا كان لهذا الأخير رصيد كاف أو دين كاف[2]. وقبل أن يقوم بالدفع، يلتزم مصدر البطاقة بالتأكد من مطابقة التوقيع الذي يظهر على الفواتير، وفي حالة عجزه على ذلك، يلتزم التاجر بهذا الالتزام، وهذا ألا يسبب تخلي مصدر البطاقة عن هذا الالتزام.

وقد نصت توصية المجموعة الاقتصادية الأوربية على التزام مصدر البطاقة بالسماح لحاملها بإخطاره في أي وقت عن ضياع البطاقة أو سرقتها منه، ويعتبر التزام أساسي في مختلف العقود [3].

---

1 - **JEANTIN Michel,** Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, Op.cit, p 126.

2 - En qualité de Mandataire du porteur, il n'est tenu de payer que si le porteur dispose d'un solde créditeur suffisant ou d'un crédit suffisant. Voir : **PEROCHON François**, Entreprise en difficulté instrument de droit et de paiement, op.cit., p 685.

3 - C'est la banque émettrice qui supporte, finalement et logiquement le risque de non paiement par le porteur, son client, mais elle perçoit à ce titre une commission proportionnelle au montant de l'opération, versée par la banque du fournisseur. Voir : Ibid, p 686.

ب- الالتزامات اتجاه التاجر أو مقدم الخدمة:

يقوم البنك مصدر البطاقة بإمداد التاجر بالأدوات والآلات لأداء الخدمة، وتتمثل أساسا في:

- الملصقات التي توضع في مكان ظاهر في محل التاجر للإعلان عن أداء الخدمة وهي استخدام البطاقات كوسيلة دفع.
- النشرات التحريرية اللازمة لتوعية التاجر والعاملين طرفه وآلة الطباعة اليدوية[1].
- إشعارات البيع، وتستخدم كمستند يوقع عليه العميل، بما يفيد استخدام البطاقة في السداد بقيمة السلعة أو الخدمة.
- يلتزم البنك بإعطاء التفويضات اللازمة للتجار بجميع العمليات التي يقوم بها، سواء كانت في أيام العمل الرسمية أو الإجازات وعلى مدار 24 ساعة.
- يقوم البنك بتحصيل المستحقات للتاجر، وذلك من خلال إشعارات البيع المقدمة من التاجر والموضح فيها قيمة العملية ورقم التفويض.
- تسجيل كافة المعاملات الخاصة بالتجار على أنظمة الحاسوب الآلي لدى البنـك بدءا من التفويضات حتى قيم الإشعارات المحصلة للقيام بدور إيجابي نيابة عن التاجر اتجاه البنوك المصدرة بالنسبة للعمليات المرتدة من تلك البنوك والعمل على إثبات أحقية التجار فيها، بناء على البيانات المسجلة بأنظمة الحاسوب الآلي من طرف البنك [2].

---

1 - وهي آلة صغيرة يزود بها اسم ورقم التاجر أو البنك الصارف ووظيفتها طباعة تلك البيانات، وكذلك البيانات البارزة الموجودة على البطاقة على إيصال الاستخدام.
ويمكن تعريف التفويض (Autorisations) على أنه ذلك الرقم الكودي الذي يتم إعطاؤه من البنك المصدر أو المنظمة العالمية لنبك الصارف، أو بنك التاجر للموافقة على عملية صرف نقدي أو شراء سلع وخدمات باستخدام البطاقة. أنظر: **نادر شعبان، إبراهيم السواح،** النقود البلاستكية وأثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، المرجع السابق، ص20-21.

2 - المرجع نفسه، ص21.

- ويسمح مصدر البطاقة (البنك) أن يسحب التاجر نقودا على حساب مدين بضمان الفواتير المستحقة على حامل البطاقة، فيحصل مصدر البطاقة مقابل ذلك على فوائد بالنسبة المتفق عليها.

كما قد يشتري مصدر البطاقة (البنك) هذه الفواتير من التجار، ويقوم بدفع قيمتها كاملة مقابل حصوله على عمولة متفق عليها، تتراوح عادة ما بين 2 و4% [(1)]، ويمكن اعتبار هذه العملية عملية تحويل الفواتير التي تنتج عنها علاقة ثلاثية الأطراف.

ثانيا: العلاقة بين مصدر البطاقة والتاجر:

تتمثل العلاقات الناتجة عن الدفع الإلكتروني علاقات قانونية ثنائية، بين كل متعاملين، فبعد دراسة العلاقة بين مصدر البطاقة وحاملها أو العميل، ندرس ثانيا العلاقة بين مصدر البطاقة (البنك) والتاجر أو مقدم الخدمة.

1- العلاقة العقدية بين المتعاملين:

كل تاجر يرغب أو يقبل التعامل بهذه الطريقة (الدفع ببطاقات الدفع والتعامل بها) عليه بالانخراط في تجمع البطاقات البنكية (Groupement des carte bancaire)، ويكون هذا الارتباط عادة لمدة غير محددة، وهذا يعني أن فسخ العقد ممكن من كلا الطرفين في أي وقت، وقد تنص هذه الاتفاقية (Convention Fournisseur) على بعـض الآثار كتوقيف النشاط أو الممارسة العادية للتاجر أو المتخلف عن بعض التزاماته يؤدي مباشرة إلى فسخ العقد[(2)].

1 - ولابد من الإشارة في هذا الصدد إلى أن الفواتير تختلف عن الكمبيالات، ذلك أن الفواتير مستحقة فعلا بينما الكمبيالات تستحق بعد فترة من زمن تحريرها، أنضر: **جلال عايد الشورى،** وسائل الدفع الإلكترونية، المرجع السابق، ص48.

2- La convention souvent appelée convention fournisseur, prévoit que certains événement affectant le fournisseur, comme la cessation d’activité ou le manquement à certains de ses obligations entraînent automatiquement la résiliation. Voir : **PIEDELIEVRE Stéphane**, Instrument de crédit et paiement, op.cit., p260 .

وهذا اعتمادا على القاعدة العامة "العقد شريعة المتعاقدين"، فيتم التعاقد بعد حصول مصدر البطاقة على الموافقة المسبقة من المنظمة الأصلية للبطاقة، على أن يتعاقد مع التجار ومقدمي الخدمات، ليحصلوا على قيمة مبيعاتهم التي تتم من خلال استخدام هذه البطاقة، عندئذ يستطيع مصدر البطاقة تحصيل قيمة هذه الفواتير من العميل لحساب التاجر[1].

2- التزامات التاجر اتجاه مصدر البطاقة:

يلتزم التاجر أساسا بما يلي:

- المحافظة على الأدوات والمستندات المسلمة له من البنك واستخدامها، ويجب عليه أن يضع الملصقات في مكان ظاهر للإعلان عن أداء خدمة الدفع ببطاقة الدفع.
- يلتزم التاجر بالبيع بموجب البطاقة بدون زياد في الأسعار عن الأسعار العادية أي كان البنك المصدر محلي أو خارجي.
- في حالة استخدام الآلة اليدوية يجب أن يلتزم التاجر بحد الاستعلام قبل إتمام عملية البيع، وفي حالة زيادة العملية عن حد الاستعلام، يجب أخذ تفويض من البنك[2].
- يجب عليه الإطلاع قبل إتمام العملية وطلب التفويض على قائمة البطاقات الموقوفة أو المطلوب سحبها من السوق، حيث يكون مسؤول عن أي عملية تتم من خلال بطاقة موقوفة الفعالية أو مطلوب سحبها[3].

---

1 - ويترتب عن هذه العلاقة حقا شخصيا مستقلا مجرد عن علاقة البنك بالعميل، فبمجرد قبول التاجر هذه البطاقة، يصبح له حق الرجوع إلى مصدر الطاقة لاستفاء ثمن ما قدمه للعميل، ولا يحق لمصدر البطاقة أن يتمسك بمواجهة التاجر بالدفوع التي يملك حق إثارتها أمام حامل البطاقة إلاّ إذا أخطر التاجر بها مسبقا، من بين هذه الدفوع، الدفع بعدم كفاية الرصيد أو يدفع بأنه تجاوز الحدود المسموح له بها. أنظر: **جلال عايد الشورة،** وسائل الدفع الالكتروني، المرجع السابق، ص47.

2 - ويعرف حق الاستعمال (Floor limit)، هو الحد المصرح به للتاجر للتعامل به بموجبه مع حاملي البطاقات دون الحصول على موافقة مسبقة من البنك، أو ما يسمى بالحد المسموح به للتاجر. أنظر: **نادر شعبان، إبراهيم السواح،** النقود البلاستكية وأثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، المرجع السابق، ص22.

3 - ويمكن تعريفها أنها قائمة تحتوي على البطاقات الموقوف التعامل بها بناء على طلب البنك المصدر، ويزود بها التاجر عن طريق البنك المتعاقد معه، ويجب الرجوع إليها عند تنفيذ عملية أقل من حد الاستعلام، خصوصا وأنه لا يتم أخذ تفويض عنها من بنك التاجر قبل التنفيذ. أنظر: **نادر شعبان، إبراهيم السواح**، المرجع السابق، ص22.

- يتعهد التاجر بقبول الدفع ببطاقات الائتمان، فيلتزم بإخبار الزبائن بتوفير خدمة الدفع الإلكتروني لديه، كما يلتزم بالتأكد من مطابقة التوقيع الذي يقوم به العميل، كما يلتزم بإرسال إلى مركز المعالجة التابع لمصدر البطاقة كافة الفواتير والسجلات الإلكترونية.

- يلتزم كذلك بدفع عمولة(commissions) لمصدر البطاقة [1].

- كما يقع على عاتق التاجر التأكد من أن البطاقة سارية المفعول لحظة قبولها، وأنها تحمل اسم حامل البطاقة بالإضافة إلى توقيعه، فإذا لم يتحقق مما ورد ذكره وورد فيه خطأ يتحمل التاجر نتيجة خطئه، ولا يتحمل مصدر البطاقة هذا الخطأ، والسبب في ذلك أنّه من الممكن أن تكون هذه البطاقة ملغاة أو موقوفا التعامل بها، فيتضح ذلك من خلال الإطلاع على الكشوفات المزودة له بالأصل من قبل مصدر البطاقة[2].

- الاحتفاظ بصور إشعارات البيع للمدة القانونية المتفق عليها في العقد بينه وبين البنك، كما يلتزم بتقديم الإشعارات إلى البنك في الميعاد المحدد للتحصيل، ويلتزم بكافة القواعد والنظم المحددة من قبل المنظمات الدولية[3].

- كما يقع على عاتق التاجر عدم تسليم حامل البطاقة أي مبالغ نقدية مقابل إرجاع البضاعة أو على سبيل السلف.

3- التزامات مصدر البطاقة اتجاه التاجر:

كما أشرنا إليه سالفا فعلى مصدر البطاقة أن يزود التاجر بسندات خاصة تستعمل لبيع البضاعة بموجب البطاقة، حيث يقيد فيها مواصفات البضاعة وقيمتها وبيانات أخرى

---

1 - Une partie de ces commissions est fixe, elle correspond aux loyer pour le matériel mis à disposition par l'émetteur, son appartenance à un ou plusieurs réseaux au service de paiement et au service garantie, une partie est proportionnelle et dépend du nombre et du montant d'opérations traitées. Voir : **PIEDELIEVRE Stéphane**, op.cit., p261.

2 - **جلال عايد الشورة،** وسائل الدفع الالكتروني، المرجع السابق، ص49.

3 - **نادر شعبان، إبراهيم السواح،** النقود البلاستكية وأثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، المرجع السابق، ص23.

ويقوم الحامل بالتوقيع عليها ووضعها فوق البطاقة وسحبها على جهاز خاص، وذلك حتى تثبت بيانات البطاقة على السند، كما عليه أن يزود التاجر بالأجهزة التي تستخدمها هذه الأخيرة في إتمام عملية البيع، والمتمثل في جهاز التفويض المباشر، والذي يستخدم للحصول على تفويض لإتمام عملية البيع، وكذلك جهاز يقوم بختم اسم ورقم التاجر ولسندات البيع [1].

إلى جانب ذلك، يلتزم مصدر البطاقة بتزويد التاجر بملصقات وإعلانات خاصة ببطاقة الوفاء لعرضها على واجهة محله التجاري، حتى تسهل رؤيتها من قبل حاملي البطاقة، ليتسنى لهم استخدام البطاقات في عملية الشراء، ويلتزم بتزويد التاجر بأسماء العملاء الذين أوقف التعامل معهم، كما يزوده بقائمة الاعتراضات التي تدرج فيها أسماء البطاقات التي ضاعت أو تم سرقتها[2].

ومن أهم التزامات مصدر البطاقة كذلك، اتجاه التاجر سداد الفواتير التي يوقعها الحامل طالما استخدام البطاقة قد تم بصورة سليمة من حامله، ولا يستطيع المصدر التنصل من هذا الالتزام بحجة عدم وجود رصيد أو معارضة الحامل، ويكون هذا الوفاء بموجب الضمان الممنوح في نطاق الاستعمال الصحيح للبطاقة، ويكون السداد على حدود المبلغ المتفق عليه بين الحامل والمصدر، دون تحميله أية مسؤولية عن الحد الزائد والذي لم يقم بإيفائه.

وتجدر الإشارة إلى أن تجاوز التاجر لمبلغ الضمان الممنوح من المصدر، يؤدي إلى فقدان الضمان حتى بالنسبة للجزء المضمون من العملية، فإذا أوفى على الرغم من سقوط الضمان فإنه يتصرف كوكيل من الحامل مكلف بسداد ديونه، أما إذا لم يحدد العقد بين المصدر والحامل الحد الأقصى المسموح به لحامل البطاقة، أو إذا جرت العادة أن

1- **نضال إسماعيل برهم،** أحكام عقود التجارة الالكترونية، دار الثقافة للنشر والتوزيع، مصر، 2005، ص108.

2- المرجع نفسه، ص109.

يسمح المصدر للحامل بتجاوز المبلغ المسموح به، فإن المصدر يظل ملزماً بالوفاء بقيمة ما تجاوزه حامل البطاقة[1].

يعتبر التزام المصدر بدفع قيمة الفواتير التزاما أصليا، ولا يتبع عقد البيع بين التاجر والعميل، ولا عقد إصدار البطاقة بين التاجر والحامل (العميل)، ودليل ذلك هو أن الشروط الواردة في بطاقات الائتمان تنص على ذلك. فتنص المادة 7 من نظام فيزا بنك الإسلامي على عدم مسؤولية البنك عن أي نزاع ينشأ بين العميل والتاجر، كما لا يتحمل البنك أية مسؤولية عن عيب أو نقص في البضائع أو الخدمات التي يحصل عليها العميل[2].

كما يجب على العميل وقف الوفاء بالعمليات التي تتم بتاريخ لاحق لتاريخ وفاة العميل، وذلك لأن البطاقة تقوم على الاعتبار الشخصي، وإذا التزم بالوفاء بعد تاريخ وفاة الحامل بالرغم من قيام الورثة بإخطاره بواقعة الوفاة، يتحمل حينئذ قيمة المبالغ التي أوفاها، كما يسأل عن الأضرار التي لحقت بالورثة بسبب هذا الوفاء، لأن خطأ البنك بالوفاء قد يرتب التزامات في ذمة هؤلاء تنقص من حقوقهم في التركة [3].

ثالثا: آلية استخدام البطاقات البنكية:

إن المظهر الخارجي لبطاقة الوفاء يوحي ببساطتها وسهولة استعمالها، إلاّ أن الحقيقة غير ذلك، فقد بلغت درجة من التعقيد، تجعل استعمالها مرهونا بضرورة تزويد

---

1 - وإذا أوفى المصدر بما تجاوز عن الحد المسموح، فيقوم بذلك بصفته وكيلا حسبما يذهب إليه البعض، في حين يرى البعض الآخر إلى أن المصدر يوفي من تلقاء نفسه، لذلك يحق له مطالبة العميل حسب فكرة الإثراء بلا سبب، لأن المصدر قام بالإيفاء بإرادته، ولا يلزم بذلك، وفي حالة عدم سداد الفواتير رغم قيام التاجر بما يستوجب عليه من التزامات تؤدي إلى إلحاق الضرر بالتاجر، فيكون المصدر مسؤولا مسؤولية عقدية، ويلزم بالتفويض، لأن المصدر غريب عن العلاقة بين التاجر والحامل، فإن المصدر يكون ملزما بالسداد للتاجر حتى ولو كانت البضائع معيبة أو ناقصة، بحيث يكون للمصدر أن يطالب التاجر بدفع المبالغ التي تكون للحامل على التاجر. أنظر في هذا الشأن: **نضال إسماعيل برهم،** أحكام عقود التجارة الالكترونية، المرجع السابق، ص109.

2 - المرجع نفسه، ص110.

3 - نفسه، الصفحة نفسها.

التجار بالتجهيزات اللازمة والقادرة على ترجمة المعلومات المشار إليها بواسطة رموز في البطاقة، حتى يتسنى لها أن تؤدي الوظيفة التي وجدت من أجلها وهي الوفاء.

ففي الجزائر مثلا يكون ذلك بطلب التاجر من شركة SATIM لتزويده بأجهزة نهاية الوفاء الإلكتروني، حيث يشترط في هذا الجهاز أن يتوفر على مجموعة من الخصائص بأن يتناسب مع التكنولوجيات والتقنيات الحديثة، سواء كان من النوع الثابت أو النقال. كما يجب أن يعمل حسب طريقتين مختلفتين، هما الطريقة المباشرة والطريقة غير المباشرة، ويؤمن عمليات البيع وعمليات السحب على جهاز الوفاء الإلكتروني(1).

ولأن بطاقة الوفاء تعتبر وسيلة لسحب النقود كذلك، فلابد من توفر شبابيك آلية للبنوك وموزعات آلية للأوراق النقدية، ليتمكن الحامل من سحب نقوده منها عند الحاجة، والتي هي الأخرى يجب أن تستجيب لأحدث التقنيات والتكنولوجيات، حتى تفيد العميل بالخدمة المطلوبة.

إن عملية تحويل ثمن البضائع والخدمات من حساب حامل البطاقة المشتري أو العميل إلى حساب التاجر البائع يتم بإحدى الطريقتين:

1- الطريقة المباشرة (On line):

تتم عملية الدفع في هذه الحالة في نفس لحظة حصول المشتري على السلع أو الخدمات المطلوبة، وتقديم بطاقته إلى التاجر المعني، الذي يمرر البطاقة في جهاز نهاية الوفاء الإلكتروني من أجل قراءة البيانات المدمجة على الشريط الممغنط، مع إدخال الرقم

---

1 - **عبد ا لبندة،** النظام القانوني لبطاقة الدفع، ص63. أنظر في السياق نفسه:
BENCHOHRA Kara, le commerce électronique en Algérie défis et perspectives, op.cit, p76.
- L’opération technique : SATIM (Société D’Automatisation des Transactions Interbancaires et Monétique : le centre de traitement interbancaire qui héberge les bases de données porteur et commerçant.
- L’opération technique gère le centre de personnalisation et par délégation des banques le centre d’autorisation et d’acceptation des transactions monétiques.

السري (Personale Identification Number ’PIN’)[1] أو (Le code confidentiel) فإذا كانت هذه البيانات صحيحة يدخل التاجر مبلغ العملية.

ويكون التاجر على اتصال مع الجهة التي تتعهد بالدفع، أي البنك المصدر تصله رسالة بكفاية الرصيد لإجراء عملية الدفع، وذلك بعد مطابقة الأرصـدة فيتم الوفاء بثمن المشتريات بتحويل المبلغ من حساب المدين إلى حساب الدائن مباشرة عن طريق عمليات حسابية، فيكون هذا الأمر بمثابة دفع فوري[2]، ولأن تسوية الديون تتم مباشرة لحظة إجراء الصفقة توفر هذه البطاقات أعلى درجة من ضمان الوفاء للتجار.

وما تجدر الإشارة إليه في هذا المقام أن مثل هذه الأجهزة أصبحت مرتبطة في أغلب دول العالم بحساب العميل مباشرة لدى البنك، والوسيلة الأساسية لدخول العميل لحسابه والتمكين من سحب وتحويل المبلغ الذي يريد الشراء به إلى حساب التاجـر وتتمثل في تقنية حديثة عبارة عن جهاز آخر مرتبط بجهاز التحويل، يسمى بجهاز الرقم السري، حيث يقدم التاجر هذا الجهاز للعميل، فيقوم هذا الأخير بإدخال رقمه السري حتى يتمكن جهاز التحويل من الارتباط التام مع حاسوب البنك، وتتم عملية مطابقة البيانات والأرصدة.

ولأن تقنية بطاقات الوفاء حديثة في الجزائر، فإن الجهة التي تقوم بمطابقة الأرصدة واستلام البيانات ومراقبتها ومعالجتها، والتأكد من صحة الوفاء الإلكتروني وإعادة إرسالها إلى التاجر هي أجهزة شركة العمليات البنكية والنقدية الإلكترونية (ساتيمSATIM) التي تشحن أجهزتها بمعلومات عن أرصدة وحسابات العملاء حاملي البطاقات، من خلال البنوك المصدرة لها.

---

1 - تتمثل البيانات في اسم العميل ورقم البطاقة، رقم حسابه، اسم البنك المصدر، وتاريخ انتهاء صلاحية البطاقة. فإذا كانت البطاقة غير مقبولة لأي سبب، كأن تكون ملغاة أو تم الإخطار بأنها مسروقة أو مفقودة، فإن الحاسوب المستقبل ستقوم بإرسال ما يفيد التاجر بوجوب عدم إتمام الصفقة، أو سحب البطاقة إذا لزم المر ذلك. أنظر: **عبد ا لبندة،** النظام القانوني لبطاقة الدفع، المرجع السابق، ص64.

2- المرجع نفسه، ص65.

في حين أنّه تم تعزيز جل أسواق العالم قد أصبحت تستخدم جهاز الرقم السري مما كان له الأثر الإيجابي في تقليص مدة التحويل، وإجراء القيود بين حسابات العملاء والتجار لمدة لا تتجاوز 15 إلى 20 ثانية، والقضاء بذلك على مخاطر سرقة البيانات المتعلقة بالعملاء [1].

2- الطريقة غير المباشرة (Off Line):

جوهر هذه الطريقة هو الاستناد إلى المعطيات والمعلومات المتعلقة بحامل البطاقة الممغنطة المعبأة على الشريحة، إذ يكون ذلك في حالة عدم وجود اتصال مباشر عبر شبكة الحواسيب بين التاجر والجهة المصدرة التي تتولى عملية الدفع، فبعد حصول المشتري على البضائع أو الخدمة المطلوبة، تتم تسوية عملية الدفع في هذه الحالة، بتقديم الحامل بطاقته للتاجر الذي يقوم بدوره بتمريرها على جهاز نهاية الوفاء الإلكتروني، ويدون من جهة البيانات اللازمة على فاتورة من عدة نسخ (3 نسخ عادة) وهي البيانات البارزة على البطاقة.

أما البيانات المضغوطة فيتولى جهاز نهاية الوفاء الإلكتروني قراءتها، ثم يثبت مبلغ الصفقة على الفاتورة ليقوم بعد ذلك حامل البطاقة بالتوقيع على هذه النسخ الثلاث للفاتورة إقرارا منه بصحة المعلومات الواردة فيها، بحيث ترسل النسخة الأصلية إلى الجهة التي تتولى السداد، بينما يحتفظ كل من التاجر والمشتري بالنسختين المتبقيتين، فلا تتم عملية التحويل مباشرة في لحظة الشراء، إنّما بعد تلقي البنك الفواتير فتقوم الجهة المصدرة بالدفع للتاجر عن طريق قيد المبلغ في الجانب الدائن من حسابه، وقيده في الجانب المدين من حساب حامل البطاقة[2] .

1- **عبد ا لیندة،** النظام القانوني لبطاقة الدفع، المرجع السابق، ص65.

2 - فيستفيد حامل البطاقة من الآجل الممنوح له لتسديد الفواتير بعد إرسالها إليه من البنك المصدر للبطاقة، إذ يعتبر هذا الآجل كحد أدنى للفترة ما بين حصول الشراء ووصول الفواتير إلى البنك، غير أن هذه البطاقة لا تعتبر في الحقيقة بطاقة ائتمان، وذلك لعدم تعهد البنك المصدر بتقديم أية تسهيلات ائتمانية لعملية حامل البطاقة، فكل ما يقوم به البنك هنا، هو تسوية الدين بين حامل البطاقة والتاجر إذا وجد رصيد دائن لحامل البطاقة. أنظر: المرجع نفسه، ص65.

رابعا : الأمر بالدفع عند استعمال بطاقة الدفع:

إن حداثة تقنية استعمال بطاقات الدفع وتعقيدها في مواجهة التاجر بثمن السلعة أو الخدمة التي يحصل عليها حامل البطاقة، واحترام الالتزام بالوفاء النهائي يفرض إتباع إجراءات معينة، فإذا كان استعمال النقود الكلاسيكية (أوراق وقطع نقدية) يسهل عملية القبض للتاجر لأنه سيقبض مباشرةً ثمن ما قدمه من مبيعات، فإن الأمر يختلف بالنسبة لبطاقة الدفع التي يقدمها بدل تقديم النقود السائلة. فتتم العملية بتمرير البطاقة في الجهاز المخصص لذلك لقراءة بياناتها والتأكد من صحتها وصلاحيتها، ويوقع العميل على الفواتير، فينصرف مع ما حصل عليه من سلع أو خدمات.

1- طبيعة الأمر بالدفع:

إن الغرض من كل تلك الإجراءات التي تبدأ بتقديم الحامل بطاقته للتاجر إلى غاية توقيعه على الفاتورة ذات النسخ الثلاثة، هو السماح للبنك المصدر بأن يحول ثمن المشتريات التي حصل عليها المشتري من حسابه إلى حساب التاجر المورد، وهذا هو الأمر بالدفع الذي يتم نتيجة استخدام بطاقة الدفع، ويعرف بأنّه: « ***أمر صادر من حامل البطاقة إلى بنكه بأن يخصم مبلغ العملية من حساب العميل المشتري، ويقيده في حساب التاجر، فإذا ما تم بالشكل الصحيح المطلوب يكون حامل البطاقة قد أوفى بدينه تجاه التاجر*** »[1] .

إن المشرع الجزائري لم يشترط أن يصدر الأمر بالدفع في شكلية محددة[2] فيمكن القول أنّه يكون صحيحا سواء صدر في شكل كتابي أو في شكل شفاهي، ويشترط في الأمر بالدفع أن يكون مرفقا بتوقيع حامل البطاقة على الفاتورة التي يقدمها له التاجر من ثلاثة نسخ، ويترتب عن ذلك أنه في حالة قيام حامل البطاقة بالمعارضة في الوفاء لدى

---

1 - **عبد ا لبندة،** النظام القانوني لبطاقة الدفع، المرجع السابق، ص66.

2 - **حميزي سيد أحمد،** تحديث وسائل الدفع كعنصر لتأهيل النظام المصرفي الجزائري، رسالة لنيل درجة ماجستير في العلوم الاقتصادية، فرع التحليل الاقتصادي، كلية العلوم الاقتصادية والعلوم التسيير، جامعة الجزائر، 2001، ص112.

البنك المصدر للبطاقة وتنتقل المسؤولية إلى هذا الأخير إذا ما أهمل مراجعة صحة التوقيع المثبت على الفاتورة أو قام بتسوية فواتير غير موقعة [1].

2- عدم قابلية الأمر بالدفع للرجوع فيه:

يمتاز الأمر بالدفع الذي يصدره حامل البطاقة (العميل) إلى البنك بميزة خاصة ومهمة جدا، وتزداد أهميته في طريقة الوفاء غير المباشرة، فإذا ما قام شخص بتسوية ثمن ما حصل عليه من مشتريات أمام تاجر يملك جهاز نهاية الوفاء الإلكتروني بواسطة بطاقة الدفع، يكون قد أعطى أمرا بدفع مبلغ الصفقة من حسابه إلى حساب التاجر الدائن أي يقيده في الجانب المدين من حسابه، وفي الجانب الدائن من حساب التاجر [2] .

لكن إذا اكتشف المشتري لاحقا أن البضاعة أو الخدمة التي حصل عليها ليست بنفس المواصفات التي طلبها، فهل بإمكانه أن يحدث تغييرا في إرادته السابقة، بأن يرفع معارضة يمنع من خلالها بنكه المصدر من تحويل المبلغ من حسابه إلى حساب التاجر؟[3].

أجابت المادة 543 مكرر 24 من القانون التجاري الجزائري عن هذا التساؤل موضحة الخاصية التي تميز الأمر بالدفع المعطى بواسطة بطاقة الوفاء بنصها على ما يلي:«***الأمر أو الالتزام بالدفع المعطى بموجب بطاقة الدفع غير قابل للرجوع فيه، ولا***

---

1 -ومن أجل تسهيل استعمال بطاقات الوفاء خاصة في حالة ما إذا طلب السلعة أو الخدمة عبر الهاتف، أو بطريق المراسلة، تتضمن العقود النموذجية المبرمة بين حاملي البطاقات والبنك المصدر، بند ينص على أن مجرد إطلاع البنك على الكشوفات التي أرسلها إليه التاجر كاف لقيام البنك بتحويل المبلغ المطلوب من حساب المدين إلى حساب التاجر الدائن وهو ما ورد في المادة 5/5 من عقد الانضمام (contrat d'adhèrent) لبنك التنمية المحلية. أنظر: **عبد ا لیندة،** النظام القانوني لبطاقة الدفع، المرجع السابق، ص66.

2- Le titulaire du compte autorise la banque à débiter son compte sur le vue des enregistrements ou des relevés transmis par le commerçant, pour le règlement des achats des biens ou des prestations de services. Voir **JEANTIN Michel, PAUL Le Cannu**, Droit commercial: instruments de paiement et de Crédit, entreprise en difficulté, 5ème édition, Dalloz, Paris, 1999, p 130.

3 - **عبد ا لیندة،** المرجع السابق، ص67.

يمكن الاعتراض على الدفع إلاّ في حالة ضياع أو سرقة البطاقة المصرح بهما قانونا،أو تسوية قضائية أو إفلاس المستفيد» [1] .

لكن المشرع الفرنسي كان سباقا في حسم هذا الموضوع، إذ نص على قطعية الأمر بالدفع في المادة 57-2 من المرسوم الصادر في 30 أكتوبر 1935، المعدل بقانون 30 ديسمبر 1991 بنصها على ما يلي: ***«الأمر أو الالتزام بالدفع المعطى بواسطة البطاقة غير قابل للرجوع فيه»*** [2].

كما نص كذلك كل من القانون الأوربي المتعلق بالاستعمال السليم للوفاء الإلكتروني، والقانون النقدي والمالي الفرنسي في مادته 132-2 على أن الأمر بالدفع المعطى بواسطة بطاقة الوفاء غير قابل للرجوع فيه، فإذا ما أصدر حامل البطاقة مثل هذا الأمر وفي شكله الصحيح كان أمره قطعيا وغير قابل للإلغاء، ولا يسمح لحامل البطاقة أن يتراجع عن أمره بالدفع بسبب نقص في البضاعة أو بسبب عيب فيها [3] .

لقد سبقت الإشارة إلى أن الأمر بالدفع لا يكون صحيحا إلا إذا كان مرفقا بتوقيع حامل البطاقة على الفاتورة ذات النسخ الثلاث، وعلى البنك المصدر أن يتأكد من شرعية وصحة هذا الأمر بالدفع، وما إذا كان صادرا عن صاحب الحساب و/أو بطاقة الدفع من خلال مقارنته مع التوقيع المثبت لديه عند إبرام العقد لأول مرة، فتوقيع الحامل على الفواتير إلى جانب تدوين رقمه السري ضروري لصحة الأمر بالدفع، لذلك نتساءل عن مدى قيام أمر بالدفع، ووجوده في الحالة التي لم يبرز الحامل رقمه السري للتاجر ولم يوقع على الفواتير التي يقدمها له هذا الأخير [4].

ويجب التمييز بين حالة مع إذا كان الدفع قد جرى باستخدام الرقم الظاهر للبطاقة فقط، أم باستخدام الرقم الظاهر والسري المضاف، حيث يعتبر هذا الأخير بمثابة توقيع

---

1 - راجع المادة 543 مكرر 24 من القانون التجاري الجزائري.

2- L'ordre ou l'engagement de payer au moyen d'une carte est irrévocable... Voir : **JEANTIN Michel, PAUL Le Cannu**, Droit commercial: instruments de paiement et de Crédit, entreprise en difficulté, Op.cit, p 129.

3 - **عبد ا لبندة،** النظام القانوني لبطاقة الدفع، المرجع السابق، ص 68.

4 - المرجع نفسه، الصفحة نفسها.

الكتروني مقبول، ويعد قرينة على تأكيد الالتزام، وعلى ذلك فإذا جاء الدفع مقتصرا على إبراز الرقم الظاهر فقط، فلا مجال لاعتبار وجود أمر الدفع مع إمكانية انتقاصه.

أما إذا حصل أن تم استعمال الرقم الظاهر على البطاقة بالتزامن مع استعمال الرقم السري لصاحبها، فإن الاتجاه السائد في معظم الدول التي أقرت قوانينها بصحة الدفع الحاصل بهذا الشكل، يميل صوب إمكانية تطبيق مبدأ عدم جواز التراجع عن أمر الدفع[1].

لكن إذا حصل الدفع بالبطاقة ووقع حاملها الكترونيا عن بعد طبقا لآلية التوثيق والتصديق، كاستخدام أدوات التشفير في التوقيع، أو أن يصادق على الدفع طرف ثالث محايد، فلا يبقى عندئذ أي مجال لاستبعاد تطبيق مبدأ عدم قابلية التراجع عن أمر الدفع وذلك باعتبار أن التوقيع الإلكتروني مماثلا للتوقيع اليدوي وحائز على نفس القوة الثبوتية[2] .

كما أن عقد الانضمام يتضمن بنداً يمكن البنك المصدر من إجراء عملية الدفع بتحويل المبلغ المطلوب من حساب المدين إلى حساب الدائن بمجرد الإطلاع على التسجيلات أو الكشوفات المقدمة من طرف التاجر، دون حاجة إلى فواتير موقعة من طرف حامل البطاقة ودون إبراز رقمه السري للتاجر.

بل أن مجرد إطلاع التاجر على الرقم البارز على البطاقة يعد كافيا لإجراء عملية الدفع في مواجهة الحامل، فما مدى صلاحية الأمر بالدفع الذي يصدر بمجرد إطلاع التاجر على رقم البطاقة التي يحملها التاجر؟ ألا يعد غياب الرقم السري والفواتير الموقعة

---

1 - **عمر خالد زريقات،** عقود التجارة الالكترونية، عقد البيع عبر الانترنت: دراسة تحليلية، دار الحامد للنشر والتوزيع، 2007، ص316.

2 - أما حالة استعمال وسائل الدفع المبتكرة عبر شبكة الانترنت كالدفع بالنقود الالكترونية أو بواسطة محفظة النقود الالكترونية، فإن الاتجاه الذي نؤيده في هذه المسألة هو إمكانية التراجع عنها طالما لم تقيد قيمتها المدنية في حساب مانح الأمر، وعدم اعتبارها نهائية إلاّ بعد أن تقيد قيمتها الدائنة في حساب المستفيد. أنظر: المرجع نفسه، ص316.

من قبل حامل البطاقة انتقاصا من الأمر بالدفع في ظل اشتراط توقيع الحامل على الفواتير لصحة الأمر بالدفع؟

لقد أجابت محكمة الاستئناف بباريس عن هذا التساؤل، مقررة بأن قيام حامل البطاقة المشتري بإطلاع التاجر على الرقم البارز على البطاقة والذي هو رقمها، يعتبر أمرا بالدفع غير قابل للإلغاء، متى تم التأكد من أن حامل البطاقة قد تعاقد وبإرادته مع التاجر فعلاً [1] .

فالبند المذكور أعلاه والمدرج في عقد الانضمام وحده لا يعتد به للقول بصحة الأمر بالدفع، لأن الحامل الذي قام بهذا التصرف القانوني، قد اتجهت إرادته إلى تحقيق الوفاء بهذه الطريقة، ولأن استعمال بطاقة الدفع أمر متفق عليه في العقد الذي يجمع البنك المصدر بحامل البطاقة.

فهذا الأخير قد أصدر أمراً بالدفع إلى البنك، وفي نفس الوقت قد التزم أو تعهد بالدفع للتاجر عند استعماله هذه البطاقة، وهذا ما يفهم من عبارة الأمر أو الالتزام بالدفع «l'ordre ou L'engagement de payer»[2] الواردة في المادة 57-2 من المرسوم الصادر في 1935 الفرنسي، والمعدل بالقانون الصادر في 1991، في المادة 57-2 والتي تشير إلى أن: ***«أمر الدفع بالبطاقة غير قابل للرجوع عنه، ولا يمكن الاعتراض على الدفع إلاّ في حالة فقدان البطاقة أو سرقتها أو في حالة التصفية القضائية للمستفيد»***[3] والتي تقابلها عبارة "الالتزام بالدفع " الواردة في المادة 543 مكرر 24 من القانون التجاري الجزائري بنفس معنى ذلك.

فيترتب على قطعية الأمر بالدفع وعدم قابليته للرجوع نتيجة هامة، مفادها أنه لا يتأثر بموت من صدر منه أو بفقدانه الأهلية، أو تم سحب البطاقة من حاملها [4].

---

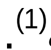
1 - **عبد ا لیندة**، النظام القانوني لبطاقة الدفع، المرجع السابق، ص 69.

2 - أنظر المادة 543 مكرر 24 من القانون التجاري الجزائري.

3 - **عبد ا لیندة**، المرجع السابق، ص 69.

4 - Voir : Article 5/4 du contrat d'adhèrent de la BDL.

من خلال ما تقدم يمكننا استنتاج الحالات التي يمكن للعميل أو حامل البطاقة الاعتراض أو الرجوع عن أمر الدفع، وهي حالة فقدان البطاقة أو سرقتها منه، أو في حالة التصفية القضائية للمستفيد. وفي هذه الأحوال يمكن لحامل البطاقة أو العميل المطالبة باسترجاع المبالغ التي دفعت من خلال هذه الحالات السالفة الذكر، ويقوم بالمعارضة على أمر الدفع الناتج عن الاستعمال غير القانوني لبطاقة الائتمان.

على عكس ما تنص عليه القواعد العامة الخاصة بأمر الدفع أو أمر التحويل التقليدي الذي يعتبر أمر قابل للمعارضة أو للرجوع فيه[1].

المطلب الثالث

التحويل المصرفي الإلكتروني

تعتبر التحويلات المالية ما بين المؤسسات المصرفية والنقدية، من أهم العمليات والنشاطات التي ترتكز عليها لتحقيق الأهداف المسطرة من طرف هذه المؤسسـات وتطبيق السياسة المسطرة منها في إطار التعاون المصرفي ما بين هذه المؤسسات.

وبتطوير الوسائط الإلكترونية وأنظمة المعلوماتية وقنوات الاتصالات، أصبحت التحويلات المصرفية الإلكترونية أكثر انتشارا، وذلك راجع إلى السرعة في تنفيذ هذه العقود والثقة ما بين المتعاملين في مجال التحويل المصرفي الذي يعتبر عملية لانقضاء التزام أصلي الناتج عن الدفع الإلكتروني ما بين المشتري الذي يستعمل وسيلة الكترونية لاقتناء حاجياته من سلع وخدمات.

فتوكل مهمة تحويل مبالغ هذه الاحتياجات للمصرف الذي يملك رصيد لديه بصفة دورية حسب الاتفاق، والبائع الذي يتعهد بقبول هذه الوسائل كوسيلة قانونية

1- Les règles du droit commun du mandat doivent être respecter, il en résulte que… l'ordre de virement est essentiellement révocable. L'ordre de virement devient irrévocable à partir de la date de son inscription au débit du compte du donneur d'ordre, l'ordre de virement devient caduc en cas de survenance d'une incapacité au de décès du donneur d'ordre. Voir :

JEANTIN Michel, Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, 4ème éditions, 2005, p86.

للحصول على مبلغ ما وفره من خدمة أو ما باعه من سلعة والذي يوكل بدوره مصرفه أو المؤسسة المالية التي يعتمد لديها بتحصيل حقوقه من جراء نشاطه التجاري.

إن تقنية التحويلات المصرفية «***هي عملية نقل الأموال من حساب مصرفي لحساب مصرفي أخر، سواء كان هذا الحساب المصرفي لنفس الشخص أو لغيره، وسواء كان ذلك في إطار بنك واحد أو بين عدة بنوك وطنية كانت أو أجنبية***»[1].

من هنا نأتي إلى تبيان ضرورة دراسة ماهية التحويل المصرفي الإلكتروني (فرع أول) ولأن المستجدات التكنولوجية وثورة المعلوماتية استحدثت إلى جانب المصارف أو المؤسسات المالية التجارية التقليدية مؤسسات ذات نفس الطبيعة، إلاّ أنّها مجردة من الطابع المادي والوجود الفعلي الملموس لها، وهذا ما يسمى بالبنوك الإلكترونية أو الرقمية، التي يكون جل نشاطها على الخط، وعبر قنوات الاتصالات ومراسلات بيانية نظرا لأهمية وضخامة المبالغ المالية التي تنتقل من وإلى كل مؤسسة مالية، خاصة مع التفتح على شبكة الإنترنت التي استغلت من طرف البنوك التجارية. [(2)]مما يستدعي دراستها (فرع ثاني).

الفرع الأول

ماهية التحويل المصرفي الإلكتروني

إذا كان تعريف التحويل المصرفي يعرف بأنه: «***عقد بين الآمر بالتحويل المصرفي والبنك مصدر الحوالة، يلتزم بموجبه البنك بأن يدفع بنفسه أو بواسطة غيره مبلغاً من النقود يعادل قيمة الحوالة إلي المستفيد من الحوالة مقابل عمولة متفق***

1- **ركروك راضية،** البنوك وعمليات تبييض الأموال، مذكر نيل شهادة الماجستير في القانون فرع قانون الأعمال، جامعة مولود معمري تيزي وزو، 2006، ص46.

2 - En 1991, 82 % des ménages réglaient leurs factures par chèques , ils n'étaient plus que 75% en 1996, alors que dans le même temps les paiement électronique (carte de crédit ou de débit, virement automatiques ont passés de 18% à 25% en France. Voir : **GRANIER Thierry** et **JOFFEUX Corynne**, Internet et transactions financières, Editions Economica, Paris, 2002, p 26.
Le taux de bancarisation dans les pays africains est l'un des plus faible au monde, s'il atteint 99 %dans certains pays industrialisés, de 50% à 60 %au Maghreb, il ne représente qu'entre 3% et 7 %dans l'union économique et monétaire ouest africaine(UEMOA). Voir : **Abdul Aziz Dia**, banque pour tous à l'horizon 2020. In www.afriqueblogue.com. Le 16 septembre 2009.

عليها»[1] أو كما عرفه القانون النموذجي للتحويلات الدولية للأموال (Model law on international credit transfert) الصادر عام 1992 عن لجنة التجارة الخارجية التابعة للأمم المتحدة المعروف بـ (UNCITRAL) الذي يعرف التحويل المصرفي بأنّه «***مجموعة من العمليات التي تبدأ بأمر الدفع الصادر عن الآمر بهدف وضع قيمة الحوالة تحت تصرف المستفيد***» [2].

فتعريف التحويل المصرفي الإلكتروني لا يختلف عن التحويل المصرفي العادي سوى بوجود وسائل اتصال الكترونية تسمح بالقيام بالعملية عن بعد، والتي تتم بعلاقة عقدية بين المؤسسات المالية.

أولا: تعريف عقد التحويل المصرفي الإلكتروني:

اهتم التشريع والفقه بتعريفه. إذ عرف قانون تحويل الأموال الإلكترونية الأمريكي التحويل المصرفي الإلكتروني بأنه: «***عملية تحويل للأموال تبدأ أو تنفذ من خلال وسيلة إلكترونية كالهاتف، الحاسوب أو شريط مغناطيسي بهدف أمر أو توجيه أو تفويض منشأة مالية بإجراء قيد دائن أو مدين في الحساب***».

ويضيف القانون، فيعرف الاتصال الإلكتروني بأنّه «***الرسالة المرسلة الكترونيا بين العميل والمنشأة المالية بصورة تسمح بعرض ورؤية النص بواسطة وسيلة عرض كشاشة الحاسوب***».

ويكاد هذا التعريف يكون التعريف التشريعي الوحيد الموجود لعقد التحويل المصرفي الإلكتروني [3].

ويرى جانب من الفقه أن الوسيلة الإلكترونية المقصودة في التعريف السابق هي الأداة الإلكترونية التي يمكن بواسطتها للعميل إجراء التحويل المصرفي الإلكتروني، ولابد لتلك الوسيلة لكي تعتبر وسيلة الكترونية أن تكون قادرة على تحرير إيصال مكتوب لكل

1 - **محمد عمر ذوابة**، عقد التحويل المصرفي الالكتروني (دراسة قانونية مقارنة)، المرجع السابق، ص23.

2 - المرجع نفسه، ص22.

3 - نفسه، ص24.

عملية تحويل مصرفية الكترونيا، وبناء عليه يرى بأن الهاتف لا يعتبر وسيلة الكترونية بالمعنى السابق[1] وتجدر الإشارة إذن إلى أنه لكي يتم تكييف عقد التحويل المصرفي الإلكتروني كذلك، أن يصدر الإيجاب والقبول عن بعد، أي دون تحقيق مجلس العقد الذي يجمع بين الطرفين.

ويمكن الإشارة في هذا المقام إلى أن الأمر رقم 03-11 المتعلق بالنقد والقرض[2] وباستقراء نصوصه لاسيما المادة 51، والتي تندرج في المحور الثالث الخاص بالعمليات التي يقوم بها البنك الجزائري، والتي تنص على أنّه «***يمكن للبنك الجزائري القيام بكافة العمليات البنكية مع البنوك والمؤسسات المالية التي تنشط في الجزائر ومع كافة البنوك المركزية الخارجية***»[3]. وبناء على ذلك يمكننا الاستنتاج أن التحويل المصرفي الإلكتروني عملية قانونية منصوص عليها في النظام البنكي الجزائري، اعتمادا على عبارة: «...**كل العمليات**...» (Toutes opérations) السالفة الذكر، والتي تعتبر قفزة نحو تطوير النظام البنكي الجزائري، وتطوير تقنيات نشاطه ما بين المؤسسات المالية والبنوك.

ثانيا: أنواع التحويل المصرفي الإلكتروني:

تتعدد صور التحويل المصرفي الإلكتروني بتعدد أطرافه أو العناصر المتدخلة لإتمامه، ويمكننا التمييز بين عدة صور، وهذا التعدد راجع إلى عدم وجود نظام أحادي

1 - لم تعد البنوك تستعمل الرسائل البريدية في تنفيذ الحوالات المصرفية سواء الداخلية منها أو الخارجية، وإنما استبدلت الرسائل البريدية بالرسائل الالكترونية عبر شبكة الانترنت أو شبكت سويفت.
وفي الولايات المتحدة الأمريكية تستخدم وسيلتان أساسيتان هما شبكة البنك المركزي الفدرالي، ونظام الدفع الخاص بغرفة المقاصة في نيويورك المعروف بـ (chips). أنظر في ذلك: **محمد عمر ذوابة**، عقد التحويل المصرفي الالكتروني (دراسة قانونية مقارنة)، المرجع السابق، ص24-25.

2 - أمر رقم 03-11 المؤرخ في 27 أوت 2003، يتضمن قانون النقد والقرض، ج ر عدد 52، الصادرة بتاريخ 27 أوت 2003.

3- أنظر المادة 51 من الأمر رقم 03-01 .والمتضمنة صلاحيات بنك الجزائر.

للعملية، وإنما يخضع أساسا لحرية التعاقد التي تتمتع بها المؤسسات البنكية[1]، وما يسمى بالعقد شريعة المتعاقدين.

1- التحويل المصرفي الإلكتروني بحسب البنوك المتدخلة في العقد:

هناك صورتان أساسيتان:

أ- التحويل المصرفي بين حسابين في بنك واحد: فيقوم البنك بخصم مبلغ الحوالة من حساب الآمر، وإضافته إلى حساب المستفيد، ويترتب عن ذلك نقص جانب أصول حساب الآمر ليزيد بنفس القدر حساب المستفيد مع ثبات مجموع أرصدة البنك، فهي عملية بسيطة تتم في لحظة واحدة بدون فارق زمني بين عملية الخصم والإضافة عند استعمال القيد عن طريق الحاسوب. وتجدر الإشارة إلى أن التحويل المصرفي بين حسابات لدى فروع البنك الواحد تعتبر حسابات لدى بنك واحد، لأن الفرع لا يتمتع بشخصية مستقلة [2] .

ب- التحويل المصرفي بين حسابين في بنكين مختلفين: وفي هذه الصورة يقوم بنك الآمر بخصم قيمة الحوالة من حساب الآمر ويقوم في المقابل بنك المستفيد بقيد قيمة الحوالة في حساب المستفيد، ومن ثم تتم عملية التسوية بين البنكين[3].

2- التحويل المصرفي الإلكتروني بحسب المستفيد:

نصت في هذا المقام المادة 1/329 من قانون التجاري المصري على أن التحويل المصرفي قد يتم من حساب إلى آخر، كلاهما مفتوح باسم الآمر بالتحويل لدى البنك ذاته

---

1 - **JEANTIN Michel,** Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, op.cit., p85.

2 - **محمد عمر ذوابة**، عقد التحويل المصرفي الالكتروني (دراسة قانونية مقارنة)، المرجع السابق، ص26.

3 - لهذه التسوية عدة طرق، فقد يكون البنكان يحتفظ كل منهما بحساب لدى البنك الآخر، وعندئذ تتم التسوية من خلال قيد الدائن أو قيد المدين لحساب أحد البنكين لدى البنك الآخر، كما قد تتم التسوية عن طريق بنك ثالث يحتفظ كلا البنكين بحسابات لديه، أو يمكن أن تتم التسوية من خلال غرف المقاصة. أنظر: المرجع نفسه، ص27.

أو لدى بنكين مختلفين. كما قد يتم بين حسابين لشخصين مختلفين في ذات البنك أو لدى بنكين مختلفين. ونستخلص مما سبق أن هذه الصورة من التحويل يمكن أن تتم بطريقتين:

- إذا قام الآمر بإجراء التحويل من أحد حساباته لدى البنك إلى حساب آخر في ذات البنك، كأن يقوم بتحويل مبلغ من أحد حساباته الدائنة لتغطية أحد حساباته المدنية لدى ذات البنك، ذلك أن الحسابات المختلفة وإن كانت لشخص واحد فإنّها تكون مستقلة عن بعضها البعض. وتجدر الإشارة إلى أنه في هذه الحالة فإن أطراف عقد التحويل المصرفي هما اثنان، الآمر وهو ذاته المستفيد من جهة، والبنك من جهة أخرى.

- تتمثل في التحويل من حساب الآمر إلى حساب المستفيد لدى نفس البنك أو لدى بنك آخر، وفي هذه الحالة يضع بنك الآمر تحت أمر بنك المستفيد (إذا كان التحويل بين بنكين مختلفين) ائتمان بمبلغ مساوي للمبلغ المراد نقله، ويقوم هذا الأخير بقيد قيمة الحوالة في حساب المستفيد وبعد ذلك تسوى العلاقة بين البنكين[1].

ولتفعيل وإنجاح هذه العمليات ذات الأهمية البالغة من الناحية الاقتصادية، والتي تسهل سيولة الأموال، يمكننا الإشارة على سبيل المثال إلى أحد الأنظمة الأوربية التي تنشط في هذا المجال، وهو نظام "TARGET".

3- نظام "TARGET" نموذج للتحويل المصرفي الإلكتروني في أوربا:

هو نظام الدفع مباشرة، أي (En temps réel) الذي يستعمل بالتحويلات التي تتم بالأورو، والذي يسير من طرف البنك المركزي الأوروبي "BCE"، ويتشكل من 16 نظام داخلي، والتابعة للدول الأوربية، وكان الغرض من ذلك هو وضع أرضية موحدة لمعالجة الدفع الخاص بالمبالغ الضخمة بالأورو، وكان يهدف أساسا إلى:

- منح ميكانيزم فعلي وفعال من أجل دفع المبالغ بالأورو ما بين الدول الأوربية[2].
- وضع همزة وصل ما بين أنظمة الدفع في مجال الاتحاد الأوروبي.

---

1 - **محمد عمر ذوابة**، عقد التحويل المصرفي الالكتروني (دراسة قانونية مقارنة)، المرجع السابق، ص27.

2 - **BOUYALA Régis,** Le monde des paiements**,** op.cit. p 103.

- تطبيق السياسة النقدية للبنك المركزي الأوربي، وترقية السوق المالية بالأورو[1].

وقد تم تطوير هذا النظام ليسمى نظام.TARGET 2 .

ولتفعيل التحويل الأسهل للأموال، سار الإتحاد من أجل المتوسط (UPM) في هذا الاتجـاه ويظهر ذلك من خلال إتحاد مجمعات بنوك أروبية وإفريقية التابعة لبعض الدول الأعضاء بهدف تسهيل التحويل المصرفي بينها سواء تعلق الأمر بالتحويلات التي يقوم بها المهاجرين أو المستثمرين بين الشمال والجنوب[2].

الفرع الثاني

البنوك الإلكترونية

أتت تكنولوجيا الاتصالات بتغيير حتى في كيان المؤسسات الاقتصادية، فأدى ذلك إلى ظهور مؤسسات مقرها الاجتماعي وجل طرق معاملتها تتم عبر شبكة الانترنت وظهر في النظام المصرفي ما يسمى بالبنوك الإلكترونية.

أولا: تعريف البنوك الإلكترونية:

يستخدم اصطلاح البنوك الإلكترونية (Electronic banking) أو بنوك الإنترنت (Internet banking) كتعبير متطور وشامل للمفاهيم التي ظهرت مع مطلع التسعينات لمفهوم الخدمات المالية عن بعد أو البنوك الإلكترونية عن بعد (Remote electronic banking)، أو البنك المنزلي (Home banking) أو البنك على الخط أو الخدمات المالية الذاتية (Self-service banking).

وجميع هذه المصطلحات تعني أن الزبون تتاح له كافة أعماله الخاصة بالبنك الذي يتعامل معه في أي مكان يكون موجود به، وذلك عن طريق خط خاص يوفره البنك[3]

1 - كما توجد العديد من الأنظمة الأوروبية للتحويلات الالكترونية للأموال، منها نظام (ABE) منذ 1998، والذي يجمع حوالي 160 بنك، والذي يتمخض عنه نظام (euro1)، (step 1)، (step 2). أنظر في ذلك:
Ibid, pp.104-108.

2 -**Pascal Airault**, l’offensive des banques méditerranéennes, jeune Afrique, no 2479 du 13 au 19 juillet 2008 , Tunisie ,p72.

3 - **منير الجنبيهي**، البنوك الالكترونية، دار الفكر الجامعية، مصر، 2006، ص10.

فهي بنوك كاملة الخدمات التي يقدمها البنك التقليدي، وإنّما الفارق أن البنك الإلكتروني لا وجود له في الواقع كمباني ومقرات اجتماعية تقليدية، وإنما مقره شبكة الإنترنت.

وذلك اعتمادا على البرمجيات الموجودة على موقع البنك في الشبكة أصبح للعميل إمكانية الدخول وقضاء كافة ما يريد من أعمال دون أي تقيد بأعمال معينة موجودة على الكمبيوتر الخاص به، وأعمال أخرى برمجياتها ليست على كمبيوترها الخاص بها [1].

تمتاز البنوك الإلكترونية بتقديم خدمات لعملائها طوال الوقت، دون التقيد بأوقات معينة كالبنوك التقليدية، أي دون أن يكون هناك إجازات للموظفين مثلا، أو غياب موظف ما، فهي تقدم كافة خدماتها في كافة أيام الأسبوع طوال ساعات اليوم الأربع والعشرين[2] وهذا راجع للتطور التكنولوجي الذي نتج عنه استعمال الكمبيوتر الشخصي (PC) الذي ساعد على تطوير النظام البنكي المتفتح على المستوى الخارجي فالمؤسسات يمكنها أن تدخل مباشرة إلى الأنظمة البنكية باستعمال الكمبيوتر الشخصي (PC) وتحويل الأموال بوساطة التحويل الإلكتروني أو التحويل بالكابل[3] أي على الخط.

فالتبادل الإلكتروني للبيانات يحتوي عادة مركبات التحويل الإلكتروني للأموال (EFT)[4] مما تقدم يمكن القول أن البنوك الإلكترونية عبارة «عن مؤسسات تقدم أو توفر الخدمات البنكية، ولا تعتبر وكالات تابعة للبنوك التقليدية، وإنّما بنوك قائمة بذاتها والتي توفر للعملاء تخفيض رسوم التحويل الكلاسيكي للأموال الذي تقوم به البنوك التقليدية»***[5]***.

1- وفي نفس المقام أصبحت تلك البنوك الالكترونية تتولى تقديم خدمة كبرى للشركات التي تبيع عبر شبكة الانترنت فيما تعرض بالتجارة الالكترونية، إذ أصبحت تلك الشركات تستخدم تلك البنوك الالكترونية من مبيعاتها من العملاء الذين يقومون بالشراء، وذلك باستخدام وسائل الدفع الحديثة أو ما يسمى بالنقود الالكترونية. أنظر: **منير الجنبيهي**، البنوك الالكترونية، المرجع السابق، ص12.

2- المرجع نفسه، ص13.

3- **SMITH Rob et SPEAKER Mark et THOMSON Mark,** Comment faire votre commerce sur internet, op.cit., p133.

4- Ibid, p133.

5- Ibid, p143.

ثانيا: مميزات البنوك الإلكترونية:

من أهم المزايا التي تتمتع بها البنوك الإلكترونية:

- ميزة الانخفاض الكبير في تكاليف خدماتها، فبعدما كان البنك يقوم بتخصيص الكثير من الأموال لفتح فروع جديدة له في كافة المناطق في محاولة التقرب من العملاء [1]، فأصبح البنك الإلكتروني في منتهى القرب من العملاء، بحيث أصبح أقرب للمتعاملين من أقرب فرع لأي بنك تقليدي، وفي نفس الوقت يقوم بكافة الخدمات التي يوفرها البنك التقليدي العادي، وعليه تم تخفيض تكاليف كثيرة من أموال وأيدي عاملة وأجهزة ومصاريف كان يتكبدها البنك التقليدي في إنشائه لفروع جديدة.
- إمكانية الوصول إلى قاعدة أوسع من المعلومات من طرف العملاء عبر العالم دون التقيد بمكان أو زمان معينين.
- تقديم خدمات مصرفية كاملة وجديدة، والتي تتماشى مع نصوص التجارة الإلكترونية[2].
- خفض تكاليف التشغيل والاستغلال بالاستغناء عن شراء الموقع (المبنى)، تأثيثه تكاليف الصيانة والعمالة وكافة المواد الاستهلاكية.
- زيادة كفاءة أداء البنوك، وذلك بتوفير السرعة في إنجاز الأعمال البنكية مقارنة بالبنوك التقليدية، فالدخول إلى موقع البنك الإلكتروني أسهل بكثير من انتقال العميل جسديا إلى موقع البنك[3]، بحيث تكون العمليات أسهل وأسرع عبر شبكة الإنترنت وشبكات الاتصال الخاصة التي تربط بين البنك ووكلائها.

1 - **منير الجنبيهي**، البنوك الالكترونية، المرجع السابق، ص11.

2 - المرجع نفسه، ص 16.

3 - نفسه، ص 17.

ويمكننا القول أنها مميزات إيجابية تبين أهمية ونوعية الخدمات التي تقدمها هذه البنوك، لصالح العملاء عبر الشبكة العنكبوتية مستثمرين كانوا أم موردين أم تجار وحتى المستهلكين،خاصة إذا وفرت القدر اللائق من الأمان والحماية للمعاملات المصرفية.

ثالثا: تكييف النظام القانوني للبنوك الإلكترونية:

مقارنة بالبنوك التقليدية، من حيث الكيان القانوني فإن البنوك التقليدية لها كيان قانوني، ولها واقع ملموس على الأرض، متمثلا في فروعها الكثيرة المنتشرة وعدد كبير من الموظفين، بينما البنوك الإلكترونية ليس لها فروع منتشرة على أرض الواقع وإنما فرع واحد يستطيع أي من العملاء الوصول إليه مهما كان مكانه، ومهما كان الوقت الذي يريد الدخول فيه إلى البنك، وكذلك البنوك الإلكترونية ليس لها هذا العدد الكبير من الموظفين الموجودين في البنوك التقليدية [1].

فمن حيث الخدمات المقدمة إلى العملاء، فإن البنوك التقليدية تقدم كافة العمليات المصرفية إلى عملائها، ولكن الطريقة التقليدية تحتاج إلى الكثير من الجهد والوقت من كل من البنك والعميل، أما البنوك الإلكترونية فهي تقدم ذات الخدمات إلى عملائها أيضا ولكن بطريقة الكترونية حديثة توفر كل هذا الوقت والجهد.

لذاك يرى البعض، أن البنوك الإلكترونية لابد وأن تخضع لذات قواعد القانونية المنظمة لعمل البنوك بشكلها التقليدي، وذلك حتى يتوفر للعملاء الحد المناسب من الطمأنينة عند قيامهم بالتعامل مع تلك النوعية من البنوك [2] ولعلّ خضوعها لرقابة البنوك المركزية على غرار البنوك التقليدية دليل على خضوعها لنفس القواعد من جهة وكذلك توفير الحماية والطمأنينة للعملاء من جهة أخرى.

---

1 - **منير الجنبيهي**، البنوك الالكترونية، المرجع السابق، ص27.

2 - المرجع نفسه، ص28.

الفصل الثّاني:

مخاطر الدفع الالكتروني والحماية منها

بعدما أحطنا علما في الفصل الأول بالأسس والقواعد التي تتم بموجبها تقنيات الدفع الإلكتروني، كتقنيات حديثة تستعمل فيها وسائل على شكل بيانات سواء تعلق الأمر بالشيك الإلكتروني أو الكمبيالة الإلكترونية كوسائل مطورة أو تعلق الأمر ببطاقات الائتمان التي تحتوي على شريط مغناطيسي معبأ بمعلومات تسمح بقراءتها بالحواسيب أو الأجهزة المعدة لذلك التي تنقل بواسطتها البيانات الشخصية الخاصة بعملية الدفع والتي يفترض حماية سريتها بحيث لا يمكن الاستغناء عنها لإتمام هذه العمليات وانقضاء التزام كل متعامل.

وساهمت ثورة المعلوماتية وتكنولوجيا الاتصالات إيجابيا في تحقيق سرعة عقد الصفقات وتحقيق الائتمان بين المتعاملين بدليل ضخامة المعاملات التي تتم بالوسائل الإلكترونية، إلاّ أن هذه التقنيات حملت في طياتها مخاطر وليدة التطور التكنولوجي بظهور ما يسمى بالجريمة المعلوماتية الناتجة عن الاستغلال غير المشروع لهذه الوسائل أي الحواسيب وقنوات الاتصال وغيرها من الوسائل الحديثة.

فلم تعد المعلوماتية مجرد وسيلة لإلحاق الضرر بالغير فقط، بل قدرتها على معالجة البيانات ونقلها، سواء في شكل منتجات أو خدمات مستحدثة أكسبتها قيمة تجارية ذات طابع مالي ما هيأ الفرصة لظهور قيم اقتصادية مستحدثة[1] فالقيمة المالية لهذه البيانات والتي يكون التعدي عليها عن بعد ينقص من فرص القبض على الجاني بحيث يتم من أي مكان بالوسائل الرقمية الحديثة. فتعتبر الجريمة المعلوماتية مفهوم يضم الجرائم التقليدية لكن تحدث عن طريق التكنولوجيا الحديثة كما تشمل كذلك على الجرائم التي ظهرت بظهور هذه الوسائل الحديثة[2]. وظهر مصطلح الجريمة المعلوماتية الذي يضم الجرائم التامة بالتكنولوجيا الحديثة من وسائل وقنوات اتصال عن بعد[3].

---

[1]- **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2004، ص136.

[2] - **Senes Diane** et **Cluzeau Anna**, la cybercriminalité nouveaux enjeux de la protection des données, mémoire de fin d'étude, université laval, lundi 15 décembre 2008, p3.
In : www.moimreonline.com

[3]-la cybercriminalité : c'est l'ensemble des infractions pénales commise sur les réseaux de télécommunication, en pratique « internet ». on distingue les infractions liées aux technologies (virus, piratage, etc…) et celles facilité par les réseaux (copie illicite de logiciels ou d'œuvres audiovisuelles, etc… voir **: le petit Larousse illustré**, Edition Larousse, Paris, 2005, p322.

وعن الاحتيال المالي عبر شبكة الإنترنت وسبل مواجهتها تدفعنا إلى ضرورة اهتمام بإدارة مكافحة جرائم التزييف والتزوير خاصة بعد أن تطور العملية المصرفية الإلكترونية دوليا ومحليا عمل على ظهور جرائم الاحتيال والنصب الإلكترونية وفي مقدمتها القضايا المتعلقة بجرائم بطاقات الدفع الالكترونية[1] (مبحث أول).

فكان من المنطقي أن تتصدى الوسائل التقنية والنظم القانونية لهذه الجرائم لهذه المخاطر قصد تأمين عملية انتقال الأموال الإلكترونية بكل سلام التي أخذت صدى في الاقتصاديات الغربية خاصة إلى حد القول بالاستغناء الكلي للدعائم الورقية والاعتماد على الانتقال الإلكتروني للبيانات.

ووضع وسائل تتلاءم وطبيعة الجريمة قصد الحد منها، ويأتي هذا الاهتمام على المستويين الدولي كاهتمام الأمم المتحدة والإتحاد الأوربي لضرورة وضع حد لهذه الجرائم والمستوى الداخلي باعتماد نصوص قانونية ردعية لمجرمي المعلوماتية والمعتدين على البيانات وذلك تحقيقا للتعاون الدولي في هذا المجال وكل هذه الحماية والتعاون من أجل حماية البيانات فرضتها أهمية المعاملات المالية عبر قنوات الاتصال خاصة الشبكة الأم الأنترنت والتي لا تعرف المفهوم التقليدي للحدود ولتفتحها على العالم ومساسها لكافة الدول والشركات مما يستدعي دراسة الحماية التقنية والقانونية للدفع الإلكتروني (مبحث ثان).

[1]- **عصمت سعد**، خسائرها بالمليارات... جريمة إلكترونية كل ثلاث دقائق على الإنترنت، مقال منشور في الموقع : www.ensan.net، الثلاثاء 22 نيسان 2008، ص1.

المبحث الأول

الجريمة المعلوماتية الماسة بالدفع الإلكتروني

أدت إزالة صفة الدعائم المادية للوسائل التي تمت دراستها في الفصل الأول والتي تعتبر وسائل معالجة إلكترونيا بحيث تظهر على شكل صور على شاشة الحاسوب وهذا يسمى بالبيانات الرقمية التي تعتبر عرضة للفعل الجرمي كالتعدي عليها بتغير مكوناتها وبياناتها لأغراض الغش والاعتداء على مال الغير أي مال المتعاملين بهذه الطرق والوسائل مما يستدعي دراسة أنواع الاعتداءات على هذه البيانات لكونها أموال منقولة والبحث عن أنماط التعدي على هذه البيانات (مطلب أول).

تتعرض البطاقات البنكية باختلافها لهذه الجريمة بصفة كبيرة بحيث يمكن الاستيلاء على البطاقة ذاتها بالحيازة والاستعمال غير المشروعين أي اعتداء مادي وكذا الاعتداء على البيانات المخزونة في الذاكرة أو الشريط المغناطيسي أو الشريحة المتواجد فيها وبالتالي ارتأينا الإلمام بالجرائم الواقعة على البطاقات البنكية نظرا لكونها الوسيلة الأكثر عرضة للجريمة المعلوماتية(المطلب الثاني).

المطلب الأول

ماهية الجريمة المعلوماتية المالية

بغض النظر عن مدى الخبرة والتفوق اللذين توصل إليهما الإنسان إلا أنه كل عمل نقوم به تعترضه مخاطر تعيق تقدمه وتطوره فتعتبر وسائل الدفع الحديثة أكثر عرضة للمخاطر من غيرها[1] لذلك وللاهتمام البالغ بالاعتداء على البيانات سندرس طبيعة البيانات في (فرع أول) لنتطرق إلى ماهية الجريمة المعلوماتية (فرع ثان) وللإلمام بالموضوع ندرس أنواع الجرائم المعلوماتية وخصائصها (فرع ثالث).

1- **جلال عايد الشورة**، وسائل الدفع الالكتروني، المرجع السابق، ص87.

الفرع الأول

الطبيعة المالية للبيانات دافع للجريمة الإلكترونية

تثير المعلومات والبيانات المتبادلة بين الحواسيب العديد من التساؤلات فهل يمكن وصف هذه المعلومات بأنها أموال؟ وهل ينطبق عليها وصف المنقول؟[1] الشيء الذي أثار بموجبه جدلا فقهي حول وقوع الجريمة المعلوماتية كما اهتمت الكثير من التشريعات بهذه المسألة قصد إعطاء التكييف القانوني الملائم لتجريم فعل التعدي على البيانات وسندرس هذه المسألة في إطار القانون المقارن قصد الإلمام بالموضوع بمختلف جوانبه.

أولا -اتجاهات وقوع جريمة النصب المعلوماتي:

ظهرت هناك عدة اتجاهات فهناك من يرى أن الجريمة المعلوماتية جريمة قائمة حين وقوعها، وهناك من يـرى غير ذلك فسارت التشريعات كل حسب الاتجاه الذي تأثرت به.

الاتجاه الأول: هذا الاتجاه يرى أن جريمة النصب لا تقوم إلا إذا خدع شخص شخصا أخر مثله وأن يكون الشخص المخدوع مكلفا بمراقبة البيانات وعلى ذلك لا يتصور خداع الحاسب الآلي بوصفه آلة، ومن ثمة لا يطبق النصب الجنائي الخاص بالنصب والاحتيال لافتقادها أحد العناصر اللازمة لتطبيقه، وهذا الاتجاه تبنته تشريعات مصر، ألمانيا، إيطاليا والسويد.

وهناك في الفقه المصري من يرى أن غش أجهزة الحاسب هو نوع من تجسيد الكذب الذي تتحقق به الطرق الاحتيالية ضمن السلوك الإجرامي في جريمة النصب ويتفق هذا الرأي مع رأي الفقه الفرنسي والبلجيكي.

1- فإذا كان موضوع الاعتداء على الأموال في نطاق المعالجة الآلية للمعلومات ينصب على الحاسب الآلي ذاته، وما يربطه من أسلاك وما يتصل به من ملحقات، فإنه هنا لا يثير أية صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال منقول مادي... أما إذا وقع الاعتداء على ما يتعلق بفن الحاسب الآلي من برمجيات Software ونظم فإن النصوص التقليدية تأتي قاصرة عن حمايتها، أنظر: **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والانترنت، المرجع السابق، ص ص 137، 139.

الاتجاه الثاني: وتتبناه الدول الأنجلوساكسونية منها بريطانيا وأستراليا وكندا وهو اتجاه يوسع من النصوص المتعلقة بالعقاب على جريمة النصب، ويمكن تطبيقها على النصب المعلوماتي، ولقد تدخل المشرع الإنجليزي عام 1983 واعتبر خداع الآلة بنية ارتكاب غش مالي هو من قبيل الاحتيال الذي يجب العقاب عليه جنائيا، وبذلك تطبيق نصوص تجريم النصب على ذلك الغش أو الاحتيال بطرق معلوماتية ولقد سار على نفس النحو القضاء الكندي والأسترالي.

الاتجاه الثالث: وتمثله الولايات المتحدة الأمريكية حيث تطبق النصوص المتعلقة بالغش في مجال البنوك والجريمة والتلغراف والاتفاق الإجرامي على حالات النصب المعلوماتي بل أن بعض القوانين المحلية في بعض الولايات الأمريكية، أصدرت في هذا الخصوص وأضفت تعريفا موسعا للأموال بأنه" **كل شيء ينطوي على قيمة**"، ومن ثم يندرج تحت تعريف هذه الأموال المعنوية والبيانات المعالجة حيث تعاقب هذه القوانين على الاستخدام غير المسموح به للحاسب الآلي بغرض اقتراف أفعال الغش أو الاستيلاء على الأموال.

وعلى المستوى الفيدرالي فقد أصدر قانون سنة 1984 يعاقب على الولوج غير المشروع والمصطنع في الحاسب الآلي ونص فيه على عقاب كل من ولج عمدا في حاسب آلي وبدون إذن أو كان مسموحا بالولوج منه واستغل الفرصة التي سمحت له عن طريق هذا الولوج لأغراض لم يشملها وقام عمدا عن طريق هذه الوسيلة باستعمال أو تعديل أو إتلاف أو إفشاء معلومات مختزنة في الحاسب، وطالما أثرت هذه الأفعال على أداء وظيفته ولهذا يرى الفقه إمكانية تطبيق هذا النص وبشروط محدودة على جريمة النصب المعلوماتية[1].

فيعتبر المحرر الرقمي حسب تعريف المنظمة الدولية للمواصفات والمقاييس (ISO) أنه" مجموعة من المعلومات والبيانات المدونة على دعامة مادية بشكل دائم بحيث يسهل

---

[1]- **محمد محرم محمد علي**، جريمة النصب والتجارة الالكترونية، مقال منشور في الموقع: www.f-law.net/law/index.php، 2007/06/08.

قراءتها مباشرة أو باستخدام آلة مخصصة ومن ذلك أيضا نستطيع القول بأن المحررات الإلكترونية لا يمكن رفضها لمجرد أنها كتابة مدونة على دعامة إلكترونية"[1].

ثانيا: سرقة البيانات الإلكترونية:

تعتبر البيانات الإلكترونية مجموعة من المعلومات المعالجة والمسجلة إلكترونيا، يتم تبادلها باستخدام نظم معالجة وبرامج معدة لهذا الغرض عبر وسيط الكتروني[(2)] وبالتالي عبارة عن محررات تم تجريدها من الدعائم المادية لها وبالتالي هل يمكن اعتبارها أموالا منقولة قصد تجريم فعل الاعتداء عليها وتزويرها؟ الشيء الذي اهتمت به كثير من الدول من خلال تشريعاتها المختلفة والتي سندرسها من خلال النقاط الآتية :

1-في القانون المصري:

يقوم جرم السرقة وفقا للمادة 311 من قانون العقوبات المصري على "**كل من اختلس منقولا مملوكا لغيره**"[(3)] ويقصد "بالشيء" وفقا لنص المادة 1/81 من التقنين المدني المصري اصطلح أن يكون محلا للحقوق المالية، قابلا للتعامل فيه" ولذلك فإن كل شيء له قيمة يكسب صفة المال، والاعتداء على المعلومات والبيانات المنسوخة ونقل الدعامات والأشرطة المضغوطة يتوافر به جرم السرقة من ثم الاستيلاء عليها ونقل حيازتها من صاحبها الأصلي إلى حيازة الجاني وهو بذلك يشمل اعتداء على منقول، إذ أن الاستيلاء على المعلومات هي هدف الجاني وليس الدعامة الفارغة[(4)] وبالإضافة إلى ما سبق بيانه، يتطلب المشرع المصري لانطباق وصف السرقة على فعل اختلاس المعلومات بدون رضاه صاحبها أن تكون هذه المعلومات أو البيانات محل الفعل مملوكة للغير.

وحتى تكتمل أركان السرقة لابد من توافر الركن المعنوي إلى جانب الركن المادي، الذي يتحقق بتوافر القصد الجنائي العام أي العلم والإرادة زيادة على ذلك توافر قصد خاص، يتمثل في انصراف نية الجاني إلى إدخال المال المنقول في حيازته الكاملة

---

[1]- **عمر خالد زريقات**، عقود التجارة الإلكترونية، عقد البيع عبر الإنترنت، دراسة تحليلية، دار الحامد للنشر والتوزيع، الطبعة الأولى، 2007، ص213.

[2]- المرجع نفسه، ص216.

[3]- **محمد أمين احمد الشوابكة**، جرائم الحاسوب والانترنت، المرجع السابق، ص144.

[4]- المرجع نفسه، ص145.

أي نية التملك والتي تتحقق بحرمان المالك الشرعي من سلطاته على المال محل السرقة والحلول محل المالك في سلطته على هذا المال[1].

2-في القانون الفرنسي:

وفقا لنص المادة 311 عقوبات فرنسي لا تقع جريمة السرقة إلاّ إذا كان الشيء محل الاعتداء مملوكا للغير" بتوافر القصد الجنائي العام طبقا للقواعد العامة- بتوافر العلم والإرادة وتتخذ صور القصد الجنائي الخاص نية التملك، وفي إطار المعلوماتية ممثلة في شبكة الأنترنت أساسا يكون الاعتداء على النظام المعلوماتي بفعل الدخول غير المشروع طبقا للمادة 1/323 من قانون العقوبات الفرنسي الجديد، أو البقاء غير المشروع في النظام المعلوماتي وارتكاب الجرائم الأخرى.

نرى أن الدخول إلى النظام المعلوماتي العام الذي يمكن أن يدخل إليه أي مستخدم بغرض الحصول على معلومات لا يقوم به جرم السرقة، ولكن انتهاك النظام المعلوماتي الخاص والمبرمج بسرقة كلمة المرور واختراق نظامه الأمني كجدران النارpare-feu هو الدليل على توافر علم الجاني بدخوله إلى نظام خاص وبالتالي توفر القصد الجنائي إضافة إلى ذلك أن تتجه إرادة الجاني إلى الاستيلاء على المعلومات وإخراجها من حوزة صاحبها وإدخالها في حوزته بنية تملكها بالتزامن مع فعل الاختلاس وإلاّ فإن الجريمة لا تقع[2].

وقد أقر الفقه الفرنسي أن انتهاك نظام الأمن يعتبر دليلا ضمنيا على وجود القصد وسوء نية مرتكب الفعل، حيث يعد هذا الانتهاك في حد ذاته وسيلة إثبات، حيث أن الدخول غير المشروع يلازم كعنصر مقترن للجريمة لفكرة الاعتداء على النظام[3] ونرى

1- **محمد أمين احمد الشوابكة**، جرائم الحاسوب والانترنت، المرجع السابق، ص148.

2- المرجع نفسه، ص161.

3- وقد أكد القضاء الفرنسي توافر ركن الاختلاس الواقع على المعلومات وذلك بتكييف المعلومة على أنها شيء، جاء ذلك في حكم لمحكمة مونبليه (Montpellier) في قضية تتلخص وقائعها في قيام مبرمج لنسخ معلومات احتفظ بها لنفسه أثناء إحدى الزيارات لمؤسسته الأولى بعد تركه لعمله فيها، حيث قررت المحكمة أن المتهم قد اغتصب هذه المعلومات والتي تتعلق بمستخدمه السابق ... وقد حكم عليه بشهر حبس مع إيقاف التنفيذ. المرجع نفسه، ص162

أن أرقام بطاقات الائتمان قد تكون عرضة للسرقة من قبل الغير وتستخدم في عمليات الدفع الالكتروني عبر الشبكة وهنا نكون بصدد جريمة احتيال.

3- في القانون الأمريكي:

حذت بعض الولايات الفدرالية حذو القانون الفدرالي الخاص بحماية أنظمة الكمبيوتر لعام 1977 (CSpA)، حيث أصدرت عدة قوانين تعرف المال بأنّه: "كل شيء يمثل قيمة" فيشمل هذا التعريف الأموال المعلوماتية والبيانات والمعلومات والكيانات المنطقية بوصفها تمثل قيمة فأي اختلاس للبيانات أو المعلومات أو الكيانات المنطقية بمعالجتها آليا فهي مجرمة تحت القانون الفدرالي[1].

وقد طبقت المحكمة الفدرالية العليا القوانين الخاصة بالسرقة على سرقة المعلومات في قضية "جيرار"، حيث تمسكت بأن بيع المعلومة التي تم الحصول عليها من عدة بيانات خاصة بالحاسب الآلي، كافية لتأييد إدانة موظف حكومي بالسرقة، إعمالا لنص المادة 641/18 من قانون العقوبات الأمريكي[2].

4- في القانون الجزائري:

فعلى غرار التشريعات سابقة الذكر، حذا المشرع الجزائري حذو التطور التشريعي الذي يستلزم أن يتلاءم التطور التكنولوجي مع تطور الجريمة المعلوماتية وكذا الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فنصت المادة 350 من قانون العقوبات الجزائري على «***كل من اختلس شيئا غير مملوك له يعد سارقا***»[3].

فهذه المادة لم تذكر إذا ما كان فعل السرقة يقع على منقول مادي فقط أو يمكن أن يشمل المنقول المعنوي أيضا لكن الفقه فصل في ذلك واعتبر أن المنقول يكون ماديا لأن فعل الاختلاس هو مادي ملموس ، حين يقوم شخص سيء النية بأخذ الشيء عنوة وبقوة أو أخذ الشيء خلسة المهم أن للفعل وجود مادي.

1- **محمد أمين احمد الشوابكة**، جرائم الحاسوب والانترنت، المرجع السابق، ص162.

2- المرجع نفسه، ص163.

3- أنظر في ذلك نص المادة 350 من القانون 82-04 المؤرخ في 13 فبراير 1982 والمتضمن قانون العقوبات الجزائري.

وكنتيجة لذلك لا يمكننا أن نتصور قيام الاختلاس في حق الأشياء المعنوية غير الملموسة وبالمقابل نصت المادة 394 مكرر من القانون نفسه على عكس ذلك :"يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"[1].

ولقد نصت كذلك الفقرة الثانية من المادة نفسها على تضاعف العقوبة في حالة حذف أو تغيير لمعطيات المنظومة وكذلك تخريب استغلال المنظومة.

كما نصت المواد التي تلي المادة سالفة الذكر على تجريم فعل الدخول بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها[2]. كما نلتمس إجراءات خاصة في التصدي للجرائم المعلوماتية في تعديل لقانون الإجراءات الجزائية والمتعلقة بالجرائم المعلوماتية والتي تنص على تمديد اختصاص وكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في بعض الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[3].

كما نصت معظم التشريعات العربية على تجريم اقتحام بطريق الغش نظاما لمعلومات حاسب آلي خاص بالغير، أو الجرائم المتعلقة بعرقلة أو إفساد عمدا تشغيل نظام حاسب آلي، من بينها القانون الإلكتروني وتكنولوجيا الاتصالات والمعلومات في فلسطين لسنة 1996[4].

من خلال القوانين المشار إليها يمكننا الاستخلاص أن التكيف القانوني للبيانات التي يتم من خلالها ميكانيزم الدفع الإلكتروني عبر الحواسيب وقنوات الاتصالات كالإنترنت

---

[1]- راجع المادة 394 من القانون رقم 04-15 المؤرخ في 27 نوفمبر 2004، المعدل والمتمم للأمر 66-156 المؤرخ في 8 جويلية سنة 1966 والمتضمن قانون العقوبات والمنشور في الجريدة الرسمية، عدد 71، 10 نوفمبر 2004.

[2]- أنظر في ذلك المواد 394 مكرر، 394 مكرر 2 من قانون العقوبات الجزائري، ج ر عدد 71، 10 نوفمبر 2004. وأنظر كذلك في نفس المنوال: **وائل أنور بندق**، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، المرجع السابق، ص1087.

[3]- **وائل أنور بندق**، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، المرجع السابق، ص1089.

[4]- المرجع نفسه، ص735.

عبارة عن أموال منقولة وبالتالي ضرورة تجريم الاستيلاء غير المشروع لها الشيء الذي دفع إلى تنظيم ووضع تشريعات ردعية تتماشى وطبيعة هذه التقنية التي تتجرد من الطابع المادي الملموس وإعطاء ثقة وضمان للمتعاملين والمستثمرين على حد سواء بضمان معاملاتهم الإلكترونية وتحويلاتهم الإلكترونية للأموال.

الفرع الثاني

تعريف الجريمة المعلوماتية

يقصد بجرائم الحاسب والإنترنت تلك الجرائم التي تطال المعرفة، الاستخدام، الثقة الأمن، الربح والمال، السمعة والاعتبار ومع هذا كله فهي لا تطال حقيقة غير المعلومات لكن المعلومات بأشكالها المتباينة في البيئة الرقمية، إن جرائم الحاسب بحق هي جرائم العصر الرقمي.

فتعرف الجريمة عموما في نطاق القانون الجنائي أنها فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا.

أما جرائم الحاسب فيعرفها مكتب تقسيم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دورا رئيسيا من هنا يمكن أن نقول بأن جرائم الحاسب هي كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"[(1)].

كما يعرف البعض الجريمة الإلكترونية الرقمية أنها" ***نشاط إجرامي تستخدم فيه التقنية الإلكترونية الرقمية و(الحاسوب الآلي الرقمي وشبكة الإنترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف***[(2)].

---

[1]- **محمد دباس الحميد، ماركو إبراهيم نينو**، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، الطبعة الأولى، عمان الأردن2007، ص60.

[2]- **مصطفى محمد موسى**، أساليب إجرامية بالتقنية الرقمية ماهيتها ... مكافحتها، دراسة مقارنة، دار الكتب القانونية، بدون طبعة، 2005، ص56.

كما نص المشرع الفرنسي في القانون رقم 19 لسنة 1988 ضمن نصوصه والخاصة ببعض الجرائم الإلكترونية (المعلوماتية) وذلك في نص المادة 2/462 والتي تنص" ***كل من توصل لنظام المعالجة الآلية للبيانات بطريق التحايل ويقصد بالتحايل تدخل غير مشروع***"[1] وقد نصت نفس المادة أن يترتب على جريمة التوصل إلى نظام المعالجة آليا للبيانات بطريق التحايل أحد الآثار الثلاثة:

- محو البيانات la suppression de données
- تعديل البيانات la modification de données
- تعطيل تشغيل النظام l'altération du fonctionnement de system [2].

ولقد ذهب تيار من الفقه إلى تعريف الجريمة المعلوماتية وهو المصطلح المترجم من الفرنسية Crime informatique والمتضمن المعالجة الآلية للبيانات، الفقهاء بأنّها: «**أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة تقنية الحاسب**» أو هي «**أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه" أو هي كل سلوك إجرامي بمساعدة الحاسب الآلي أو تحدث في محيطه»[3].**

وفي موقف منظمة التعاون الاقتصادي والتنمية (OCDE) في تعريفها للجريمة المعلوماتية تنص أنّها «***كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية***».

ومن التعريفات السابقة نجد أن الجريمة المعلوماتية تستهدف في جوهرها المعلومات بمفهومها الواسع من بيانات ومعلومات وبرامج تطبيقية وتقوم هذه الجريمة على اعتبارين مهمين أولهما أن تكون المعلوماتية وسيلة للغش والتحايل والاعتداء والثاني أن تكون المعلوماتية نفسها محلا للاعتداء[4].

1- **مصطفى محمد موسى**، أساليب إجرامية بالتقنية الرقمية ماهيتها ... مكافحتها، دراسة مقارنة، المرجع السابق، ص57.

2- المرجع نفسه، ص 58.

3- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، دون طبعة، الإسكندرية 2007، ص 115.

4- المرجع نفسه، ص116.

كما يمكننا الإشارة إلى عدة محاولات فقهية لوضع تعريف للجريمة المعلوماتية فعرفها اتجاه أن المقصود بها "الاعتداءات التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".

ويرى اتجاه آخر أنّها مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب.

ويعرفها الفقيه الألماني" **تاديمان**" الجرائم المعلوماتية بأنّها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب"[1].

فيمكننا الاستخلاص من هذه التعاريفات المذكورة أن الجريمة المعلوماتية "هي التي يكون موضوعها النظام المعلوماتي أي البيانات نفسها التي تتداول عبر قنوات الاتصال مما يعرض الشيك الإلكتروني والكمبيالة الإلكترونية كوسائل الدفع معالجة الكترونية لخطر التزوير والغش وغيرها من الجرائم والتي سيتم التطرق إليها فيما يلي وبفضل خصوصية مهارة المجرم المعلوماتي يمكنه اقتراف هذه الجرائم بالمعالجة الدقيقة غير المشروعة لهذه البيانات.

الفرع الثالث

خصائص الجريمة المعلوماتية

إن طبيعة المعالجة الالكترونية للبيانات جعلت من المخاطر والجرائم التي تتعرض لها ذات طابع خاص وبالتالي يمكننا تمييزها عن غيرها بتبيان خصائص الجريمة المعلوماتية:

أولا- ترتكب من مجرم غير عاد:

فإذا كان المجرم المعلوماتي يتوافق مع المجرم التقليدي بكونه إنسان اجتماعي، فإنّه يتميز عنه من حيث المعرفة والمهارة والوسيلة الخاصة بهذه الجريمة وهذا الاكتساب يتم عن طريق الدراية المتخصصة في هذا المجال حيث يتمتع بالذكاء، إذ أنّه يستغل ذكاءه في

1- **محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، دون طبعة، الإسكندرية، مصر، 2004، ص44.

تنفيذ جريمته أي أن المجرم من ذوي المستويات العلمية غالبا[1] سعيا لتحقيق الربح من جراء تنفيذ جريمته عاديا.

ثانيا- جرائم المعطيات ناعمة مغرية للمجرمين:

فإذا كانت الجرائم التقليدية تحتاج من مرتكبيها إلى قوة عضلية لتنفيذها فإن جرائم المعطيات لا تحتاج إلى مثل تلك القوة العضلية وإنّما إلى قوة علمية وقدرة من الذكاء ومهارة في توظيف ذلك، والجاني في سبيل تنفيذها لا يحتاج من الوقت إلا ثوان أو دقائق معدودات ونعومة هذه الجريمة وما تدركه من أرباح ومن إشباع للفضول عند البعض جعلها من الجرائم المغرية والجذابة للمجرمين[2].

إن صفة المرونة والتكيف التي تتميز بها الجريمة المعلوماتية العابرة للحدود الجغرافية بين الدول، جعلتها تنتهز كل الفرص المتاحة أمامها لكسب الربح المادي وبالتالي فإن التقدم التكنولوجي والعلمي الذي شهدته السنوات الأخيرة ساهم في ضخامة الجريمة المعلوماتية، كقرصنة البرامج المعلوماتية وجرائم شبكة الانترنت التي أخذت بعدا كبيرا في السنوات الأخيرة، حيث يعتبر هذا النوع من الجرائم من الآثار السلبية التي خلفها التطور التكنولوجي المعاصر، كما تسهل هذه التكنولوجيا الحديثة الأعمال غير المشروعة لمرتكبيها.

تمثل الجرائم المعلوماتية أبرز الصور الحديثة التي تعرفها الجريمة المنظمة عبر الوطنية، ويصعب في هذا الإطار إيجاد تعريف جامع ومانع للجرائم المعلوماتية، ويعود ذلك إلى خشية حصرها في مجال ضيق، خاصة بالنظر إلى سرعة التطور الذي يعرفه هذا المجال.

كما يصعب تعداد أو حصر كل أنواع الجرائم المعلوماتية نظرا لازديادها وتنوع أساليبها، إلاّ أنّه تعتبر القرصنة من نسخ برامج معلوماتية وأفلام ومواد موسيقية، ونشرها على شبكة الانترنت من أهم هذه الأمثلة، وهي جرائم داخلة في مجال التعدي على الملكية الفكرية إلى جانب التعدي على البطاقات الائتمانية والمصرفية، خاصة وأنّها ظاهرة

[1]- **محمد علي العريان،** الجرائم المعلوماتية، المرجع السابق، ص36.

[2]- المرجع نفسه، ص37.

أصبحت عالمية يصعب التحقق فيها بسبب عدم توافر الأدلة المادية فيها، كما تعود هذه الصعوبة إلى عدم مواكبة هذه الظاهرة بإيجاد تعاريف واضحة ومحددة، وتشريعات مناسبة لها.فمجال المعلوماتية مجال دائم التطور بعيدا عن الرقابة المؤسساتية للدول دون إطار قانوني يضبطه[1].

ثالثا- جرائم المعطيات جرائم عابرة للحدود:

ليس هناك في عالم اليوم حدود تقف حاجزا أمام نقل المعطيات بين الحسابات الآلية المتواجدة في مختلف دول العالم عبر شبكات المعلومات فيمكن في بعض دقائق نقل كم هائل من المعطيات بين حساب وآخر رغم بعده آلاف الكيلومترات، كما يمكن أن تقع الجريمة من جاني في دولة معينة على المجني عليه في دولة أخرى في وقت يسير جدا، لاسيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت خاصة في مجال التجارة الإلكترونية وازدياد اعتماد البنوك عليها.

وتثير الطبيعة الدولية لهذه الجرائم العديد من المشاكل كمشكلة السيادة والاختصاص القضائي وقبول الأدلة المتحصل عليها في دولة ما أمام قضاء دولة أخرى، ولهذا فمكافحة هذه الجرائم تتطلب تعاونا كثيفا بين الدول وتوافقا كبيرا بين تشريعاتها[2] وفي هذا المجال يمكننا ذكر قضية RN Tompson وفيها قام مبرمج إنجليزي يعمل لدى بنك بالكويت بالتلاعب في معطيات بنظام الحاسب الآلي الخاص بالبنك، وذلك عن طريق الخصم من أرصدة العملاء ثم الإيداع في حسابه الخاص.

وبعد عودته إلى إنجلترا طلب من البنك تحويل الحساب الخاص إلى عدة حسابات بنكية في إنجلترا فقام البنك بذلك، أنسبت للفاعل تهمة الحصول على أموال الغير بطريق الاحتيال فحكم عليه بعقوبة السجن.

بعد استعراضنا لأهم عناصر الجريمة المعلوماتية، يمكننا إسقاطها أو تطبيق مبادئها وتكييفها كذلك في حالة تزوير الشيك أو الكمبيالة الإلكترونية نظرا لطبيعة غير

1- **سامية قرايش،** التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية، مذكرة لنيل درجة الماجستير في القانون فرع "تحولات الدولة"، جامعة مولود معمري، تيزي وزو، 2009، ص ص55 -56.

2- **محمد خليفة،** الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة للنشر، مصر، 2007، ص37.

مادية أي عبارة عن بيانات تنقل عبر قنوات الاتصال وأساسا الإنترنت. وتمس هذه الجريمة أساسا مستعملي الشيكات الإلكترونية على الخط ونتج عن ذلك الملايين من الضحايا التي تتعامل أساسا على الخط، وقد تمت أول شكوى في فرنسا في هذا المقام في سبتمبر 2004 وقد أخذ التزوير بعدا كبيرا مع مرور الوقت، رغم الحملات التحسيسية التي قام بها المختصون .

وترى الجبهة الفرنسية لمستعملي البنوك أن هذه الجريمة التي تحدث منذ 2003 تقريبا في فرنسا دفعت إلى رفع 250 شكوى تمس 30.000 شخص وقد اتخذت هذا التهديد بجدية حيث كثفت من إخطار مستعملي تلك التقنية وكذلك إبراز مسؤولية البنوك في ذلك وهذا بالقيام بعملية الخصم أو دفع الشيك الإلكتروني قبل التأكد من صحة الشيك نفسه[1] وعلى البنوك إخطار المتعاملين معها بهذه التقنية كما فعلت Société Générale عندما حدث وإن مسها تزوير على الخط في 2004. وتجدر الإشارة أن الصعوبة تمكن في الوصول إلى مرتكبي هذا النوع من الجرائم التي يكون مرتكبيها في بلد أجنبي عادة وإلى حد الساعة 95% من قضايا التزوير للشيكات الإلكترونية قد قام اقترافها من نيجيريا[2].

الفرع الرابع

أنواع الجرائم المعلوماتية في مجال الدفع الإلكتروني

إن الدفع الإلكتروني الذي يتم بالوسائل الإلكترونية، كالحواسيب وعبر قنوات الاتصال المفتوحة على كافة المتعاملين والمستخدمين لها أدت نفسها إلى تعريض هذه التقنية للعديد من الجرائم والتي سنذكر منها:

أولا-الالتقاط غير المشروع للبيانات:

وهي عبارة عن دخول غير مشروع إلى نظام معلوماتي معين كالنظام الخاص بالبنوك أو البائعين ويتمكن المجرم المعلوماتي من التقاط البيانات الشخصية للمتعاملين

1- **Myriam Berber**, une fraude aux faux cheque de banque, article publier sur : www.rfi.fr/actufs/articles/065/article-36301.asp

2- Ibid, p2.

عبر قنوات الاتصال بعد ذلك، إما عن طريق التجسس المعلوماتي أو عن طريق الاحتيال (الخداع) (Le spoofing)[1].

وتنفذ هذه الجريمة بأنماط عديدة كالتجسس المعلوماتي، ويتمثل هذا الأسلوب في قيام قراصنة الأنترنت باستخدام البرامج التي تتيح لهم الإطلاع على البيانات والمعلومات الخاصة بالمتعاملين على شبكة الإنترنت كالمؤسسات والشركات التجارية ومن ثم استخدام هذه البيانات والمعلومات في ممارسة الأنشطة الجنائية ويمكن أن تكون معلومات سرية تجارية (اقتصادية)[2].

ونرى أن المشرع الأردني قد نص في المادة 76 من قانون الاتصالات رقم 13 لسنة 1995 على أن كل من اعترض أو أعاق أو زور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل ... من هنا يتبين أن الأفعال المجرمة تقضي بالضرورة إلى الإطلاع على محتوى هذه الرسائل المتبادلة مما يشكل بالتالي فعل الالتقاط غير المشروع لها والتي قد تؤدي إلى استخدام البيانات أو المعلومات التي يتضمنها للقيام بأفعال غير مشروعة[3].

فيعاقب إذا ما تم اعتراض بريد إلكتروني (E-mail) يتضمن بيانات متعلقة بأرقام حساب بنكي أو أرقام بطاقات ائتمان أو بيانات أخرى وتم استخدام هذه البيانات في إجراء تحويلات الكترونية للأموال غير مشروعة، فإن ذلك الفعل يعاقب بنص المادة 76 من القانون المذكور.

---

[1]- **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والانترنت، المرجع السابق، ص166.

[2]- المرجع نفسه، ص 167.

[3]- في الولايات المتحدة الأمريكية- صودق على قانون التجسس الاقتصاديEA Economic Espionnage في عام 1996، وبموجبه أصبحت من الجرائم الفدرالية أن تأخذ أو تنقل أو تحصل على معلومات سرية تجارية بدون رضاه مالكها.

فقد تم إدانة شخصين في الولايات المتحدة الأمريكية بتهمة انتهاك قانون الاحتيال وإساءة استخدام الكمبيوتر CFAA، وتجب القانون الفدرالي لاحتيال التجسس وتشريعات نقل الأموال بين الولايات وكان المتهمون قد احتالوا بطريقة غير شرعية على شركة بيل ساوث Bell South من خلال سرقة نصوص ملفات الكمبيوتر والتي تحتوي على معلومات بأموال خاصة افتراضية تقدر بـ800.000 دولار، موضوعة في 911 نظام إذ تم نقل المعلومات على شكل رسائل إخبارية للمتهمين أنظر: **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والانترنت، المرجع السابق، ص168.

وهناك ما يسمى أيضا بتشمم كلمات السر وجمعها والتقاطها، فإذا كانت أنشطة الاعتداء التي تتم باستعمال كلمة السر تتم غالبا عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما أو شيوع اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسري أو محيط العمل أو حياتهم الشخصية.

فيمكن الجاني استخدام برمجيات تمكنه من تشمم أو التقاط كلمات السر من خلال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة.

وفي كل اتصال بالشبكة تجري مراقبة وتتبع حركات الاتصال حتى يطبع المستخدم كلمة السر أو اسمه، فإن البرنامج (الشمام) يجمع هذه المعلومات وينسخها إضافة إلى أن أنواعا من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها معا، كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها[1'].

ثانيا-انتحال شخصية المتعامل الشرعي بالبيانات:

يسميها البعض جريمة الألفية الجديدة، في أمن المعلومات وذلك نظرا لسرعة انتشار ارتكابها خاصة في الأوساط التجارية وتتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية وتهدف إما لغرض الاستفادة من مكانة تلك الهوية أي هوية الضحية أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى[2].

فتعتبر هذه الجريمة قيام شخص باستخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحياته، هذا الانتقال يمكنه القيام بذلك عن طريق المعلومات التي تتعلق بتلك الشخصية كالاسم والعنوان ورقم الهوية مثلا، والتي يحصل عليها من الإنترنت ويمكن أن تؤدي هذه الجريمة إلى استنزاف رصيد الضحية في البنك أو السحب

---

[1]- **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، 2007، دون طبعة، ص44.

[2]- وهذا من أكبر سلبيات الإنترنت الأمنية وللتغلب على هذه المشكلة فقد بدأت الكثير من المعاملات الحساسة على شبكة الإنترنت كالمعاملات التجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة وهذا من أكبر سلبيات الإنترنت الأمنية وللتغلب على هذه المشكلة فقد بدأت الكثير من المعاملات الحساسة على شبكة الإنترنت كالمعاملات التجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة: أنظر: **عمرو عيسى الفقي**، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، 2006، دون طبعة، ص ص102-103.

من البطاقات الائتمانية ... وكثيرا ما يقوم المجرم بتغيير العنوان البريدي للضحية إلى عنوانه كي يستقبل بنفسه الفواتير والمطالبات.

كما يمكن للانتحال أن يمس بشخصية المواقع الذي يعتبر أشد خطورة ويقوم الفاعل بهذه الجريمة من خلال وضع نفسه في موقع بيني، بين البرنامج المستعرض للحاسب الخاص بأخذ مستخدمي الإنترنت وبين الموقع Web، ومن هذا الموقع البيني يستطيع حاسب المجرم أن يتصرف وكأنه صاحب الموقع الحقيقي، ويستطيع مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع نفسه كما يستطيع سرقة هذه المعلومات أو تغييرها[1].

وقد نص قانون العقوبات المصري على تلك الجرائم في المواد من 155 إلي 159 إلاّ أنّه يرى البعض أهميتها ضعيفة رغم ما يترتب عنها من أضرار هامة سواء مادية أو أضرار معنوية للشخص الذي تم انتحال شخصيته[2].

وإلى جانب ذلك هناك صور عديدة من الغش أو التزوير الإلكتروني للبيانات ومن بينها: تغيير المحرر بالإضافة أو الحذف ويقصد بها كل تغيير مادي يدخله الجاني على المحرر بعد قيام تحريره سواء اتخذ هذا التغيير صورة إضافة كلمة أو عبارة أو رقم أو توقيع أو حذف شيء من ذلك أو إبداله بغيره.

كما قد يتم التزوير بالإضافة مثلا زيادة رقم على رقم المبلغ المثبت في المحرر[3] سواء كان هذا المحرر على بياض أو تمت إعادة معالجته بعد تمام الاستحواذ عليه على الشبكة حيث تكون المراسلة بين المتعاملين الشرعيين (البنوك، البائع، المشتري) ويتم تغيير محتواه قصد تحقيق غرض معين، كما يمكن أن يكون التزوير أو الغش كوضـع أو

---

[1]- **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص47.

[2]- المرجع نفسه، ص48

[3]- **عمرو عيسى الفقي**، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المرجع السابق، ص103.

تغيير إمضاء أو ختم ببصمة صحيحة[1].

ويكون ذلك بأن ينسب فعل الجاني إلى شخص لم يصدر عنه ذلك أن ظهور إمضاء شخص أو ختمه أو بصمة في محرر يعني أن ما يتضمنه صدر عنه هذا الإمضاء وما في حكمه هو رمز الشخصية ودليلها.

ويقع التزوير المعلوماتي بهذه الطريقة متى تم إدخال التوقيع أو الإمضاء أو البصمة بطريقة الماسح الضوئي على مستند معالج أو محفوظ داخل الحساب الآلي وتصبح الوثيقة[2] وكأنّها موقعة وممضاة من قبل صاحب التوقيع أو الإمضاء أو البصمة ويكون الحصول على هذا التوقيع أو البصمة عن طريق المباغتة أو الغش على صحاب البصمة أو الإمضاء[3] الالكتروني دون رضا هذا الأخير.

ولقد تم النص على ذلك في قانون العقوبات الجزائري في القسم السابع الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات وفي الفقرة الثانية من المادة 394 مكرر والتي[4] تنص «تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة... ببيانات المحرر الالكتروني الأصلي».

1- **عبد الفتاح بيومي حجازي**، الجريمة في عصر العولمة، دار الفكر الجامعي، مصر، 2007، ص125.

تتعدد الجريمة المعلوماتية فنجد كذلك ما يلي:

Le hameçonnage, une forme d'usurpation d'identité d'entreprise (Phishing), il s'agit a la pèche de renseignement personnels dans un étrange d'utilisateurs sans méfiance c'est l'envoi massif d'un faux Couriel apparemment authentique, utilisant l'identité d'une institution financière d'un site commerciale connu dans lequel on demande aux destinataires … de remettre a jours coordonnées bancaires ou personnelles en clinquants sur un lien menant vers un faux site web. Voir : **Senes Diane Et Cluzeau Anna**, la cybercriminalité nouvelle enjeux de la protection des données, op-cit, p5.

2- **عبد الفتاح بيومي حجازي**، الجريمة في عصر العولمة، المرجع السابق، ص126.

3- **وائل أنور بندق**، موسوعة القانون الالكتروني وتكنولوجيا الاتصالات، المرجع السابق، ص1087.

أنظر في ذلك: نص المادة 394 مكرر من قانون العقوبات الجزائري المعدل والمتمم عام 2004.

4- **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص33.

المطلب الثاني

الاستعمال غير المشروع لبطاقة الدفع

تعتبر بطاقات الدفع من أكثر وسائل الدفع الالكتروني المستعملة حديثا والتي من خلالها يسعى المتعاملون (البنوك والمؤسسات) لترقية مستقبل النقود الالكترونية، إلا أنها ونظرا لأهميتها تعتبر أكثر عرضة للاستعمال غير المشروع أو السطو على محتوياتها وحديثا قد تكون البطاقة ذاتها في آن واحد، بطاقة سحب وإيفاء مع رمز سري خاص لإجراء كل من العمليتين وهذا قد يخفف[1] من الاستعمال الاحتيالي إلا إذا أهمل الحامل المحافظة على الرمز السري[2] غير أن صور إساءة استعمال بطاقة الدفع كثيرة نتناولها فيما يلي تحليله.

يضع بعض الفقه تعريفا للاستخدام غير المشروع لبطاقة الدفع الالكتروني بأنّه "عندما يخل الحامل بشروط عقد إصدار البطاقة، يؤدي هذا إلى فسخ ذلك العقد، أو قفل الحساب الذي تقوم البطاقة بتشغيله، حيث يسأل الحامل جنائيا لمجرد امتناعه عن رد البطاقة أو استمراره في استخدامها بعد إلغائها من البنك المصدر لها، أو استمراره في استخدامها بعد انتهاء مدة صلاحيتها".

ويعاب على هذا التعريف محدوديته حيث أنه يتناول حالة واحدة من حالات الاستخدام غير المشروع لبطاقة الدفع الالكترونية وهي حالة الاستخدام غير المشروع من قبل الحامل، ولم يتناول الحالات التي تتم من قبل التاجر والغير والمصدر في بعض الأحيان.

لذلك يرى البعض أنه لا يمكن وضع تعريف للاستخدام غير المشروع لبطاقة الدفع الالكتروني وتحديد ماهيته تحديدا دقيقا ولنميز الاستخدام غير مشروع لابد من تبيان تعريف الاستخدام المشروع وشروطه.

---

[1]- **بيار إميل طوبيا**، بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، منشورات الحلبي الحقوقية، دون مطبعة، 2000، ص57.

[2]- المرجع نفسه، ص58.

فيمكن القول أن الاستخدام المشروع للبطاقة هو الاستخدام الذي يتم بواسطة الحامل الشرعي والبطاقة صحيحة (أي سارية المفعول) وفي الغرض المخصص لها وفي حدود سقفها).

شروط الاستخدام المشروع للبطاقة البنكية:

- أن يكون استخدام البطاقة من قبل حاملها الشرعي.
- أن تكون البطاقة صحيحة وغير مزورة أو تم التلاعب بها.
- أن يكون استخدامها خلال مدة صلاحيتها وسريانها وفي حدود سقفها[1].

الفرع الأول

الاستعمال غير المشروع لبطاقة الدفع من قبل حاملها

إن طبيعة بطاقة الدفع التي تنوب عن موظفي البنك بتأدية العمليات المصرفية من سحب النقود، وتحويل الأرصدة شجع بعض محترفي النصب والتزوير على الدخول في مجالها واستخدامها على التجار والبنوك، كما قد تشجع هذه البطاقة عميلها الشرعي نفسه على استعمال طرق احتيالية لاستخدامها والاستفادة منها.

أولا- الحصول على بطاقة الدفع بمستندات مزورة:

الأصل أن الحصول على بطاقة الائتمان يتم طبقا للقواعد المعمول بها في البنك مصدر هذه البطاقة وحسب المستندات المطلوبة، وبشرط أن تكون مستندات صحيحة وليست مخالفة للحقيقة، فلا يجوز أن يتقدم طالب بطاقة الائتمان بأسماء منتحلة وعناوين وهمية، أو أي ضمانات غير حقيقية وإلا تعرض للعقوبات الجنائية فضلا عما قد يتحمله البنك من خسائر نتيجة استخدام البطاقة في شراء السلع والخدمات بمبالغ كبيرة ثم يقوم

---

[1]- **أمجد حمدان الجهيني**، الاستخدامات غير مشروعة لبطاقات الدفع الالكتروني من قبل الغير، مركز الدراسات القضائية، مقال منشور في: www.coiss.com/replay.php، المملكة الأردنية الهاشمية، ص4، 2009/06/01.

حامل البطاقة بالتهرب من التزاماته، فلا يستطيع البنك الاستدلال عليه، فيضطر إلى دفع قيمة المستحقات الناتجة عن استعمال طالب البطاقة بمستندات مزورة[1].

وتقوم هذه الجريمة لما يتقدم الجاني إلى البنك بمستندات شخصية مزورة منتحلا فيها صفة الغير أو بيانات غير صحيحة ويصدر البنك له بطاقة صحيحة يستخدمها في شراء سلع وخدمات ولا يتمكن البنك من استرداد قيمتها بعد ذلك، إما لعدم الاستدلال على صاحب البطاقة وإما لأن الضمانات غير كافية.

وفي إحدى القضايا، حدث أن قام أحد البنوك برفع –دعوى جنحة مباشرة- ضد أحد الأشخاص استنادا للمادة 336 عقوبات مصري، يتهمه فيها بالاستيلاء على مبلغ 459.90 دولار ومبلغ 7904.30 جنيها تخص البنك نفسه، وذلك لأنه قام بإتباع طرق احتيالية وذلك لأن المدعي عليه استخرج من البنك المدعي بطاقة "فيزا كارد" لاستخدامها في السوق[2] المحلية، بعد أن قدم مستندات تثبت دخله السنوي لا يقل عن مبلغ 24000 جنيه مصري، حتى يتم خصم قيمة المشتريات منه شهريا فضلا عن تعهده بعدم استخدام البطاقة ما لم يكن رصيده كافيا طبقا للعقد المبرم بينه وبين البنك. [3].

ولم يقم بسداد مشترياته إلى التجار الذين رجعوا على البنك بوصفه ضامنا له، قام البنك بالسداد، وطالب بعقاب المدعي عليه بوصفه قد استعمل طرقا احتيالية تمثلت في إتمام البنك بالمخالفة للحقيقة، أنه ملئ ولديه ضمانات كافية [4] كما أنه هناك نوع آخر من الأساليب غير المشروعة يقوم بها بعض حاملي البطاقات الملغاة نتيجة عدم استعماله للبطاقة بالشكل الجيد، فقد يرغب الشخص في استخراج بطاقة ائتمانية جديدة ولكن لا يستطيع، نظرا لتاريخه الائتماني السيئ لدى جبهات إصدار البطاقات، فيذهب إلى بعض العصابات الإجرامية والتي تطلق على نفسها عيادات الإصلاح الائتماني «Credit repair

---

[1]- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص 164.

[2]- المرجع نفسه، ص 165.

[3]- وجاء في مذكرة البنك المدعي أن المدعي عليه قد تمكن من إيهام البنك بطرق إحتيالية، وعدم كفاية رصيده السنوي لتغطية مصروفات مشترياته.. فقام التاجر بالرجوع على البنك بوصفه ضامنا لحامل البطاقة، المرجع نفسه، ص165.

[4]- **عبد الفتاح بيومي حجازي**، الجريمة في عصر العولمة، المرجع السابق، ص167.

« clinics حتى يتمكن طالب البطاقة من استخراج بطاقة ائتمان دون اعتراض البنك المصدر، بعد تغيير المستندات التي تدل على سوء استخدامه للبطاقة من قبل[1].

ثانيا- استعمال البطاقة بعد انتهاء مدة صلاحيتها:

قد يقوم العميل حامل البطاقة باستعمالها في الوفاء بقيمة مشترياته لدى التجار على الرغم من عدم صلاحياتها للاستعمال، بعد إلغائها من قبل البنك المصدر، أو بعد حلول تاريخ انتهاء صلاحيتها.

ويساهم في إمكانية وقوع هذين الفرضين استغلال العميل للفترة الزمنية الواقعة بين قيام البنك بإجراء عملية إبلاغ التجار على البطاقة الملغاة أو المنتهية صلاحيتها وإحاطة التاجر علما بهذا الإلغاء الأمر الذي يترتب عليه التزام البنك بالوفاء للتاجر بقيمة مشتريات العميل.

ثالثا- استعمال الحامل لبطاقة ملغاة:

تحتفظ البنوك المصدرة بحقها في إلغاء البطاقة الممنوحة للعميل حاملها في أي وقت ودون الرجوع إلى الحامل، وذلك ضمن شروط العقد المبرم بين البنك المصدر والعميل حامل البطاقة لذلك فكل مخالفة من الحامل لهذا الشرط العقدي يرتب مسؤولية مدنية في ذمته.

كما يمكن للحامل أن يستعمل هذه البطاقة الملغاة في السحب من الموزعات الآلية في حين أن البنك لم يقم بإعادة برمجة ذاكرة الموزع الآلي، ومن ثم لم يقم بالاحتفاظ بالبطاقة أو حجزها في الآلة مما يساعد الحامل على الحصول على مبالغ نقدية دون وجه حق.

---

[1] - **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص ص168-167 .

وبالرغم أن النسبة العالمية لتقديم مستندات مزورة لاستخراج بطاقة ائتمان، قد يشكل نسبة صغيرة بالنسبة لجمالي الاعتداءات الواقعة على البطاقة، إلاّ أنّها تتزايد في الفترة الأخيرة بسبب إمكانية تزوير وثائق ومستندات الشخصية بجودة وسهولة، حقق هذا النوع من الاحتيال عام 2001 ما يقارب من 6% من إجمالي الخسائر الناتجة عن الاعتداءات الخاصة ببطاقة الائتمان مقارنة بـ 1% عام 1994.

هذا ما يثير التساؤل في مدى إمكانية إسناد جريمة النصب وبحقها في إلغاء البطاقة الممنوحة للعميل حاملها في أي وقت ودون الرجوع إلى الحامل، وذلك ضمن شروط العقد المبرم بين البنك المصدر والعميل حامل البطاقة لذلك فكل مخالفة من الحامل لهذا الشرط العقدي يرتب مسؤولية مدنية في ذمته. باعتباره قد استخدم طرقا احتيالية في مواجهة البنك من خلال التاجر، خاصة وأن إلغاء البطاقة يؤدي إلى خلع صفة الحامل الشرعي عن العميل.

ولقد جزم الفقه باستناد جريمة النصب إلى تصرف العميل المتمثل في الاستعمال غير المشروع للبطاقة الملغاة وانطلق هذا الاتجاه من نقطة استعمال العميل للبطاقة الملغاة، فاعتبرها صفة غير صحيحة حيث أن مجرد تقديم الحامل للبطاقة الملغاة إلى التاجر من أجل الوفاء لثمن مشترياته يكون قد أقنعه بوجود ائتمان وهو لا وجود له طالما أن إلغاء البطاقة مرهون بغلق الحساب[1].

فيكون تصرف التاجر بتسليم المشتريات على أساس أن هذا المشتري هو حامل شرعي لبطاقة صحيحة وهي لم يعد لها أي قيمة قانونية بمجرد إلغائها من طرف البنك الذي يخلع عنها قيمتها وكأداة وفاء، فالحامل إذن قد لجأ إلى الاحتيال من أجل الحصول على مال الغير وبسوء نية[2].انطلاقا من نقطة استعمال العميل البطاقة الملغاة ، ولم يعد للبطاقة أي قيمة قانونية بمجرد إلغائها من طرف البنك الذي يخلع عنها صفتها كأداة وفاء، فالحامل لجأ إلى الاحتيال من أجل الحصول على مال الغير بدون وجه حق وبسوء نية[3] فيمكن اعتبار ذلك اختلاس في حق البنك الضامن.

ويمكن أن يفرط حامل في استعمال البطاقة البنكية التي تكون في حوزته وهو ما يسمى بالإفراط في استعمال البطاقات البنكية (L’utilisation abusive de la carte)**.**

---

[1]- **عبد ا لبندة**، النظام القانوني لبطاقات الدفع، المرجع السابق، ص134.

[2]- المرجع نفسه، ص135.

[3]- **سعودي محمد توفيق**، بطاقة الائتمان والأسس القانونية الناشئة عن استخدامها، دار الأمين للنشر، الطبعة الأولى، 2001، ص118.

تسمح بطاقة الاعتماد لحاملها بأن يتمون بحاجيات استهلاكية دون أن يستعمل النقود الفورية مجبرا المصرف على دفع نفقاته معتمدا على الائتمان الذي يضمنه هذا الأخير بموجب عقد الانخراط الموجود بينهما.

بالطبع يكون حسابه مدينا ولكن إذا كان سيء النية فهنا يكون إما غير قادر أو ليست لديه نية تعويض المصرف عما قام بإيفائه، ولإجبار الحاملين سيئي النية على الدفع حاولت المصارف ملاحقتهم بجرم النصب والاحتيال ببعض القرارات التي برأت الحامل وبعضها الآخر جرمه وإقرار مسؤوليته[1].

فإذا كانت النفقات التي أجراها الحامل سيء النية تتجاوز المبلغ المضمون، وإذا تجاوزت لا يدفع المصرف للتاجر لعدم وجود رصيد كاف في حساب الحامل، بالنسبة لهذا التاجر يكون جرم الاحتيال قائما ذلك أن استعمال البطاقة يشكل مناورة احتيالية تهدف إلى إيهام المورد بوجود اعتماد أو حساب وهمي[2].

أما بالنسبة للتجاوز في عمليات سحب الأموال من الصرافات الآلية، ففي لبنان مثلا فإن البطاقة التي تعطي لعملاء المصرف لا تخولهم بسحب أموال تفوق تلك الموزعة في حسابهم فلا مجال لأن تطرح مشكلة التجاوز في سحب النقود.فعادة ما ترخص البنوك في اتفاقية البطاقة البنكية،المبرمة بينها وبين زبونها تجاوز حد الائتمان.

ويمكننا الإشارة على سبيل المثال إلى اتفاقية بطاقة ماستر كارد للبنك التجاري الكويتي التي تنص في أحد بنودها:

أن أي تحويل يتجاوز الحد الائتماني الممنوح للعميل يتطلب إجراء اتصال بين التاجر المستفسر والبنك...لذلك يوافق العميل على تأجيل استعماله للبطاقة إذا كان سوف يترتب على هذا الاستعمال تجاوز الحد الائتماني المتفق عليه لحين الحصول على موافقة البنك التجاري بواسطة تبادل الاتصالات.

---

[1]- **بيار إميل طوبيا**، بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، المرجع السابق، ص67-68.

[2]- المرجع نفسه، ص70.

أما في فرنسا فالمشكلة المطروحة والتساؤل الذي جرى في هذا الإطار، وهل التجاوز في السحب يعتبر احتيالا؟ وهل استعمال البطاقة وفقا للأصول العادية الطبيعية يشكل المناورة الاحتيالية المعاقب عليها قانونيا؟ فليس هناك رأي مستقر في الاجتهاد الفرنسي، أما بالنسبة لجرم السرقة فهو غير محقق لأن المصرف هو الذي يضع الأموال بتصرف المستفيدين أما الغرفة الجنائية لمحكمة التمييز الفرنسية في قرار لها اعتبرت أنّه مع انتفاء النص، هذه السحوبات لا تشكل جرما جزائيا بل تحال كإخلال بالتزام تعاقدي إلا أن القانون المتعلق بالغش المعلوماتي الصادر في فرنسا ميز بين حالتين[1].

- إما أن يعمد الحامل إلى الاستفادة من الموزع الآلي وفقا للأصول العادية الطبيعة الصحيحة ولا يكون عرضة لعقاب جزائي.
- وإما أن يلجأ إلى أفعال قصدية ومناورات غير آبه لحقوق الغير ويكون عندها للمساءلة الجزائية التي يختلف وصفها بحسب خطورة الأفعال المقترفة[2]، فالقانون يعاقب كل من أعاق أو غير (بمعنى زور) عمل الجهاز.

وإلى جانب الصور السابقة والتي يسيء حامل البطاقة استعمالها، فإن صورا أخرى لإساءة استعمال الحاسب الآلي قد تقع منه على سبيل المثال:

- تجاوز حد السحب بالتواطؤ مع الموظف أو التاجر.
- التحايل على نقاط البيع العاملة خارج الخط.
- استخدام خدمات نقاط البيع الالكترونية في إيداع شيكات بدون رصيد تضاف قيمة الشيك إلى قيمة الحساب الأصلي للعميل لتحصيل هذه الشيكات بواسطة نقطة البيع الالكترونية، قبل تمام المقاصة بين البنوك بعضها البعض[3] وهذا الاعتداء الأخير يمكن أن يشكل جريمتين الأولى هي جريمة الشيك بدون رصيد، وحامل البطاقة

---

[1]- **بيار إميل طوبيا**، بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، المرجع السابق، ص70. أنظر في السياق نفسه، اتفاقية بطاقة ماستر كارد للبنك التجاري الكويتي، ملحق1، أنظر: **مصطفى كمال طه، وائل أنور بندق،** الأوراق التجارية ووسائل الدفع الالكترونية، المرجع السابق، ص361.

[2]- المرجع نفسه، ص71.

[3]- **عبد الفتاح بيومي حجازي**، الجريمة في عصر العولمة، المرجع السابق، ص71.

يعلم بذلك، فيتوافر القصد الجنائي أما الثانية فتقع بأسلوب التحايل بصرف القيمة دون أن تتم المقاصة بين البنوك أي قبل أن يكتشف البنك المصدر ذلك.

والحقيقة أنّه كما ذكرنا آنفا فإن اختلاف التوصيفات في جرائم بطاقة الائتمـان يدعو للحاجة إلى استصدار تشريع لكافة الاحتمالات التي يمكن أن تحدث للاعتداء على البطاقة دون ترك الأمور للاجتهادات في توصيف الجرائم[1].

ففي القانون الإيجابي فإن المسألة تم حلها، فإذا كانت البطاقة سائرة المفعول أو الصلاحية فلا يوجد خطأ جنائي، فتجاوز الحد المسموح به يعتبر فقط خطأ مدنيا فالموظف أو البنك يمكنه استرجاع البطاقة وتحريك دعوى مدنية لتحميل العميل مسؤولية ذلك التجاوز[2].

أكثر من ذلك يبقى مشكل التعسف في استعمال البطاقة بالدفع، فإن استعمال بطاقة ملغاة أو منتهية الصلاحية، تمثل احتيالا في حق البائع الذي لم يخطر بذلك من طرف البنك... فحامل البطاقة الذي يطلب منه استرجاعها إذا كانت ملغاة أو منتهية الصلاحية إذا رفض ذلك سيتعرض لمتابعة قضائية بخيانة الأمانة (Abus de confiance)[3].

وقد جاء في أحد أحكام محكمة النقض الفرنسية في هذا الشأن أن استيلاء حامل البطاقة على مبالغ تتجاوز رصيده بوضعها في أحد أجهزة التوزيع الآلي المعدة لذلك لا تشكل أية جريمة جنائية وأيدت محكمة النقض الفرنسية هذا الحكم حيث جاء في حيثيات حكمها نظرا لأن محكمة الاستئناف ومن أجل الحكم ببراءة المتهم أثبتت أنّه لكي يتمكن المتهم من إجراء السحوبات بصفته صاحبها، واعتمادا على ذلك بررت محكمة الاستئناف حكمها، إلاّ أنّه في الواقع، فإن الوقائع المنسوبة للمتهم تنطوي على عدم ملاحظة أي التزام تعاقدي، ولا تندرج تحت أي نص جنائي[4].

---

[1] - **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص181.

[2] - **Ch. Gavalda** , **J. Stoufflet**, droit du crédit , effets de commerce, chèques , cartes de paiement et de crédit, édition litec, Paris , 2eme édition, 1991, p 479.

[3] - Ibid, P479.

[4] - **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والانترنت، المرجع السابق، ص195.

رابعا- امتناع الحامل عن رد البطاقة بعد طلبها من البنك:

تعتبر العلاقة ما بين العميل وبين البنك مصدر البطاقة الائتمانية هي علاقة تعاقدية تبقى بطاقة الائتمان بموجبها ملكا لمصدرها (البنك) الذي يعهد إلى العميل استعمالها عند طلب البنك ذلك بناء على عقد ساري المفعول.

ويمثل استخدام العميل للبطاقة الائتمانية بعد أن يتم الإعلان بسحبها وامتناعه عن ردها تبديد الشيء ثم تسليمه على سبيل عارية الاستعمال، وهو ما يشكل اختلاسا تقوم به جريمة خيانة الأمانة، ويكفي لتوافر الاختلاس أن ينكر الحامل وجود البطاقة في حيازته لكي يتخاص من التزامه بالرد ولا يشترط قيامه باستعمالها رغم مطالبة البنك لها[1].

الفرع الثاني

الاعتداء على نظام البطاقات البنكية من الغير

تتكون أطراف بطاقة الائتمان عادة من حاملها الشرعي البنك المصدر والتاجر الذي يتعامل معه صاحب البطاقة.

فالمقصود بالغير هنا الأشخاص دون ما سبق من أطراف التعامل بالبطاقة، وهم الذين ليسوا أطرافا في العلاقة ويقوم الغير بالتزوير، السرقة أو النصب[2].

أولا- تزوير بطاقة الدفع:

لقد جرمت المادة 1/323 من قانون العقوبات الفرنسي المساس بأنظمة المعالجة الرقمية للبيانات والتي بدورها يمكن الاعتماد عليها لردع بعض الممارسات غير الشرعية الماسة باستعمال بطاقات الدفع المستعملة بنظام معتمد على أجهزة وميكانيزم إلكتروني.

1- **المرجع نفسه**، ص197.

2- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص187.

ولقد تم التأكد على ذلك من طرف محكمة الاستئناف بباريس في 6 ديسمبر 2000، كما يوجد في قانون النقد والمال تجريم خاص والمتعلق بالممارسات الإجرامية الماسة باستعمال بطاقات الدفع في نص المادة L163-4 [(1)].

كما تم التأكد من ذلك في قانون 15 نوفمبر 2001 أضاف لقانون النقد والمال للمادة L163-4-1 والتي وسعت من الأفعال المجرمة إلى صنع، الاستحواذ، ترك، منح أو وضع تحت تصرف الغير الوسائل والبرامج الرقمية أو كل البيانات والخاصة بالاستعمال بتزوير بطاقات الدفع كما يعاقب على مجرد محاولة القيام بهذه الممارسات[(2)].

فيتم التزوير عندما تفقد بطاقة الائتمان من العميل، أو تسرق منه فيتلقاها الغير ويقوم باستبدال ما بها من بيانات ومعلومات ويقوم باستخدامها في عمليات الشراء والسحب فيشكل اعتداء ليس على البنك المصدر للبطاقة فحسب ولكن يمتد الاعتداء ليشمل حامل البطاقة أيضا هذا الاعتداء يشكل في رأي جمهور الفقهاء جريمة تزوير على اعتبار التزوير هو تغيير الحقيقة وتغيير ما على الشريط الممغنط الخاص بالبطاقة يعد تزويرا لأنه يغير ما على البطاقة من بيانات ومعلومات[(3)].

وتتم هذه العملية عن طريق ما يسمى بعملية (Skimming Devis) للحصول على خصائص الهوية الإلكترونية من القطاعات المغناطيسية من إحدى البطاقات الصحيحة، ثم نقلها بنفس الخصائص إلى بطاقة أخرى.

وتزوير البطاقة الائتمانية ذاتها قد يكون كليا وقد يكون جزئيا، حيث يتم التزوير الكلي باصطناع البطاقة بالكامل وتقليد ما عليها من كتابات وحروف وعلامات وأشرطة أو من خلال بيانات بطاقة صحيحة يتم الحصول عليها بتصويرها فوتوغرافيا بعيدا عن

---

[1]-**Ch. Gavalda, J. Stoufflet,** Droit du crédit, effets de commerce chèques carte de paiement transfert de fonds, Ed. litec, 6eme édition, 2006, p389.
La falsification ou contrefaçon de carte de paiement ou de retrait l’usage en connaissance de cause de titre ainsi trafiques, ainsi que l’acceptation en connaissance de cause de tels titres sont punissable pénitent, art. L163-4 du code monétaire et financier.

[2] -Ibid, p 389.

[3]- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص188. في نفس المرجع توجد العديد من تقنيات التزوير منها: Skimming Devise، Inposing، Scannar وعملية الصقل أو Buffer أو استعمال قارئ الكتروني مغناطيسي Electronic Magnitic Reader.

أعين العميل، وقد يكون بتغيير بعض بيانات البطاقة كنزع الشريط الممغنط الأصلي ووضع الشريط الخاص بالفاعل القائم بعملية التزوير[1].

وكل هذه الحالات والأنماط لا تدخل في حيز تعريف الفقه للتزوير بحيث يعترف بأنه: تغيير الحقيقة في محرر بإحدى الطرق التي ينص عليها القانون تغييرا من شأنه إحداث ضرر ومقترن بنية استعمال المزور فيما أعد له.

وإذا كان تعريف الفقه ينطوي على التزوير في المحررات المادية الملموسة، فإن التزوير في مجال المعالجة الآلية للبيانات عبر شبكة الإنترنت يعد من أخطر طرق الغش التي تقع في هذا المجال، ولاسيما بحلول الحساب الآلي والمحررات الإلكترونية محل الأوراق في كافة المجالات، مما يزيد من صعوبة اكتشاف وإثبات التزوير الذي يقع في هذا المجال.

وتزوير بطاقات الائتمان في نطاق شبكة الإنترنت والمعلوماتية تأخذ صورة تزوير أرقام بطاقات ائتمان خاصة ببنك معين، من خلال تزويد الحاسب بالرقم الخاص بالبنك مصدر البطاقة بواسطة برنامج تشغيل خاص[2].

ثانيا- أنواع التزوير:

هناك نوعين من التزوير الوارد على المحررات، تزوير مادي وتزوير معنوي. فالتزوير المادي هو الذي يمس المحرر وشكله، ويترك له أثرا يمكن أن يدرك بالحواس وقد يتبين هذا الأثر بالحواس المجردة، كما قد لا يظهر إلا بالاستعانة بالخبرة الفنية، فالتزوير المادي إذن هو الذي يمكن القطع بحدوثه إذا فحصنا ما يتضمنه المحرر من هذه المظاهر في الكشط أو المحو أو الطمس أو تقليد خط الغير أو نسبة كتابة أو إمضاء إلى غير صاحبها.

[1] - **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص192.

[2] - **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والانترنت، المرجع السابق، ص 201.

أما التزوير المعنوي فهو الذي يتحقق بتغيير مضمون المحرر أو ظروفه أو ملابساته دون المساس بشكله أو بياناته المادية، ولا يتخاف عنه أي أثر تدركه الحواس أو يستدل بها عند العبث بالمحرر أو الصك[1].

وتجدر الإشارة إلى أن التغيير الذي يعتد به في تزوير بطاقة الوفاء هو التزوير المعنوي الذي يغير حقيقة البطاقة من خلال تغيير المعلومات الواردة على البطاقة واستبدالها بما يغايرها ويخالفها شرط ألا يعدم ذاتية البطاقة أو قيمتها كمحو كل البيانات الموجودة عليها أو شطبها بحيث تصبح غير مقروءة، وعليه نتساءل عن مدى اعتبار التغيير الواقع على البيانات الإلكترونية المثبتة على الشريط الممغنط تزوير في محرر؟ فيذهب غالبية الفقه إلى عدم انطباق نصوص التزوير التقليدية على التعديل أو التغيير الواقع على المعطيات والبيانات المختزنة بشكل غير مرئي في كونها بيانات الكترونية ومغناطيسية وحجته في ذلك كالآتي:

أن تزوير البيانات المخزنة بشكل الكتروني لا يمكن أن ينطوي تحت النصوص التقليدية لأن هذه الأخيرة إنما تفترض إمكانية القراءة البصرية لمحتويات المحرر المدونة فيه، وهذا غير متحقق بالنسبة للمعطيات الإلكترونية المخزنة على شريط ممغنط.

إن تغيير الحقيقة الذي يقع على البيانات المعالجة الكترونيا أي كان الوعاء المحفوظة فيه لا يمكن أن تقوم جريمة التزوير بمفهومها التقليدي لانتفاء الكتابة، فطبيعة البيانات المسجلة على الشريط المغناطيسي المعالجة بطريقة الكترونية لا تسمح بقراءتها ولا التعرف بصريا على دلالتها لذاك لا يمكن اعتبارها كتابة.

إن البيانات المثبتة على الشريط المغناطيسي للبطاقة لا تتيح فرصة قراءتها إلا بجهاز معد لذلك وهي الآلة القارئة، لذاك فالمعالجة الالكترونية لهذا النوع من البيانات لا يعبر عن فكرة بشرية وإنما مجرد فكرة إلكترونية لهذا النوع من البيانات.

وبخلاف المشرع الجزائري نجد أن حماية بطاقة الوفاء من التزوير الذي حضيت باهتمام المشرع الفرنسي، وذلك بموجب نصوص خاصة، ما دام أن أغلب الفقه اتجه إلى

---

[1] - **عبد ا ليندة**، النظام القانوني لبطاقات الدفع، المرجع السابق، ص140.

عدم اعتبار التغيير الذي يقع على البطاقة وعلى بياناتها تزويرا بالمفهوم المنصوص عليه في قانون العقوبات، خاصة بالنسبة للبيانات المشفرة، مما يجعل تدخل المشرع بنصوص جديدة وملائمة ضرورة حتمية لحماية البطاقات الالكترونية من هذه الجريمة المتفاقمة[1].

ثالثا- استعمال الغير لبطاقة دفع مزورة أو مسروقة:

إن منتحل الصفة سارق كان أم مزور والذي يستعمل البطاقة لسحب الأموال من الموزعين الالكترونيين للأوراق النقدية معاقب جنائيا ومسؤول مدنيا اتجاه الضحايا (البنك والعميل صاحب البطاقة) جراء هذا الاختلاس[2] وفي جميع الحالات فإن سرقة البطاقة أو ماكينة السحب يعد اختلاسا لمنقول مملوكا للغير بنية تملكه طبقا لنص المادة 311 عقوبات مصري[3].

فتختلف جريمة تزوير المحررات عن جريمة استعمال المحررات المزورة فهما جريمتان مستقلتان عن بعضهما البعض، وجريمة استعمال المحررات المزورة إنما يقصد بها دفع هذه المحررات إلى التعامل وفي مجال بطاقة الوفاء قيام الجاني باستعمال بطاقة دفع مزورة في الحصول على السلع والخدمات لدى التاجر المورد، ثم إن العقاب على استعمال محرر مزور وارد حتى ولو لم يكن المستعمل هو نفسه المزور وأيضا يعاقب المزور حتى ولم يعقب فعله هذا استعمال المحرر المزور[4].

---

[1]- لقد تناول المشرع الجزائري جريمة التزوير في المحررات في الفصل السابع من الباب الأول من الكتاب الثالث من الجزء الثاني من قانون العقوبات تحت عنوان التزوير، وقد تناول القسم الثالث من هذا الفصل موضوع تزوير المحررات العرفية أو التجارية أو المصرفية في المادة 219 من قانون العقوبات "كل من ارتكب تزوير بإحدى الطرق المنصوص عليها في المادة 216 في المحررات التجربة أو المصرفية أو شرع في ذلك يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500 إلى 2000دج، أنظر: **عبد ا لبندة**، النظام القانوني لبطاقات الدفع، المرجع السابق، ص ص141-143.

[2] **-Ch. Gavalda, J. Stoufflet,** Droit du crédit, effets de commerce chèques carte de paiement transfert de fonds, op-cit, p480.

[3]- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص197.

[4]- فثار جدل فقهي حول طبيعة جريمة استعمال بطاقة الدفع فذهب فريق إلى تكييفها أنّها جريمة سرقة باستعمال مفتاح مصطنع وذلك على أساس أن البطاقة المزورة تدخل في مفهوم المفتاح المصطنع، وذهب فريق آخر إلى تكييف استعمال بطاقة دفع مزورة من قبل الغير جريمة نصب، فإذا ما قدم هذا الشخص البطاقة المزورة للتاجر يكون قد أوهمه بصحة هذه البطاقة مما يؤدي بالتاجر إلى الاعتقاد بوجود رصيد وهمي لهذا الحامل غير الشرعي للبطاقة المزورة. أنظر كذلك: **عبد ا لبندة**، النظام القانوني لبطاقات الدفع، المرجع السابق، ص144.

رابعا-الاعتداء على نظام بطاقة الدفع من موظفي البنك:

إن خطر الاعتداء على وسائل الدفع الالكتروني بواسطة البطاقات لا يتوقف عند الحامل أو الغير الذي يسرق أو يعتدي على نظامها، وإنّما قد يصل مرتكبي هذه الاعتداءات إلى موظفي البنوك التي تقدم خدمة الدفع بهذه الطرق ويكون بتواطؤ الموظف بالأشكال التالية:

- مساعدة العميل على استخراج بطاقة ائتمان ببيانات مزورة.
- السماح للعميل بتجاوز حد سقف البطاقة من السحب.
- السماح للعميل باستعمال بطاقة منتهية الصلاحية أو بعد صدور قرار بإلغائها[1].

ففي الحالة الأولى يكون موظف البنك هو الذي ساعد العميل على قبول المحرر المزور، بحيث يستطيع أن يسهل له عملية الحصول على البطاقة الائتمانية والتساؤل يثار هنا حول مسؤولية موظف البنك عما إذا كان فاعلا معه في الجريمة أم شريكا؟

فالمادة 39 من قانون العقوبات المصري تنص على: "يعد فاعلا للجريمة من يرتكبها وحده أو مع غيره، ومن يدخل في ارتكابها إذا كانت تتكون من جملة أعمال فيأتي عمدا عملا من الأعمال المكونة لها"، وبتطبيق هذه المادة على حامل البطاقة وموظف البنك نجد أن موظف البنك قد انطبق عليه الوصف القانوني في كونه ارتكب جريمة مع صاحب البطاقة فضلا عن ذلك فإن عمله طبقا للفقرة الثانية من المادة 39 يكون متمما لهذه الجريمة فموظف البنك على علم بأن الأوراق المقدمة من العمل مزورة.

فتواطؤ موظف البنك في استخراج بطاقة دفع بوثائق وبيانات مزورة تتعدد تكيفاتها تلك الأفعال لاعتبارات ثلاثة:

- اعتبار موظف البنك فاعلا أصليا في جريمة التزوير إذا قام هو بتدوين ما هو على غير الحقيقة في المحرر الخاص بالبنك وهو عالم بذلك.

---

[1]- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص288-289.

- اعتبار موظف البنك شريكا في جريمة التزوير إذ ساعد العميل على قبول البنك المصدر للبطاقة للمستندات المزورة المطلوبة ويتمكن من استخراج البطاقة الائتمانية.
- اعتبار موظف البنك مستعملا لمستندات مزورة، وإخفاء طابع الشرعية عليها وهو عالم بتزويرها.

أما الحالة الثانية قد يتفق موظف البنك مع العميل على إعطائه مبلغا معينا نظير علمه بالمحرر المزور لاستخراج بطاقة الائتمان، أو نظير تجاوز حد البطاقة للسحب، أو انتهاء صلاحيتها أو صدور قرار بإلغائها، وقد يتفق مع الموظف على اقتسام المبلغ فيما بينهما، فأي وصف قانوني ينطبق على أفعال الموظف في نسب هذه الجرائم المختلفة عما إذا كان هذا الوصف سرقة أو نصب أو خيانة أمانة أو رشوة؟

فلا تنطبق أركان السرقة والنصب على هذا الفعل ولا تنطبق كذلك أركان الاختلاس ولا تحايل ولا عقد من عقود الأمانة، ولكن اتفاق موظف مع العميل نظير فائدة يحصل عليها يعد من قبيل الرشوة(1).

كما يحتمل أن يكون اتفاق موظف البنك مع التاجر على الاعتداء وهي حالة تجاوز حد السحب في صرف قيمة إشعارات البيع أو حالة اعتماد إشعارات بيع منسوبة إلى بطاقة وهمية أو مزورة أو منتهية صلاحيتها أو مسحوبة، ويكون هذا الاتفاق نظير فائدة معينة تعود على موظف البنك، بالرغم أن تجاوز حد السحب قد لا يشكل جريمة في بعض الأحيان مثل إذا كان العميل مستمرا في معاملاته مع البنك، إلاّ أنّه قد يسمح للعميل باستعمال البطاقة متجاوزا حد السحب بالاتفاق مع التاجر رغم علمه بعدم كفاية الرصيد فتتوافر جريمة الرشوة بتوافر الركن المادي للجريمة في الحصول على الفائدة أو المنفعة التي تعود على الموظف، من السماح للتاجر بتجاوز حد سحب البطاقة المتعاملة معه(2).

الفرع الرابع

1- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص ص291-292.

2- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، المرجع السابق، ص294-295.

الأخطاء الفنية التي يرتكبها التاجر

وهي عبارة عن أخطاء يرتكبها التاجر أثناء عملية الوفاء بواسطة البطاقة.

أولا- عدم انتباه التاجر لاختلاف ثمن البيع والقيمة المدونة:

في الحقيقة أنه رغم قيام التاجر بارتكاب هذا الخطأ فإن نتائجه تبقى على عاتق الحامل، سواء أكان فارق الثمن لصالح الحامل، أم ضارا به، لأن توقيع الحامل أسفل الفاتورة يعد موافقة منه على القيمة المدونة أعلاه، ويستطيع التاجر تسليم نسخة الفاتورة التي بحوزته إلى المصدر لوفائها وسوف يقوم هذا المصدر بوفاء القيمة، ولن يكشف الحامل هذا الخطأ، إلاّ عند استلامه لكشف الحساب الشهري (Card Statement)، وفي ظل غياب النصوص التشريعية فإن الذي يحكم ويحدد آثاره هو عقد الانخراط الذي بموجبه تصدر البطاقة البنكية.

فينص هذا عقد حامل البطاقة المصرفية عن اعتماد ليون في فرنسا على أن الأمر الصادر من الحامل غير قابل بالرجوع فيه ما عدا حالة من حالات المعارضة طبقا للمادة العاشرة، ولن يعتد البنك الرجوع في الأمر المسبب بالنزاع التجاري بين حامل أو مالك الحساب والتاجر، حيث يبقى البنك على أي فرض من الفروض أجنبيا عن هذا النـزاع كما نص عقد الحامل لبطاقة الداينرز كلوب في فرنسا على أن:... كما أن وجوب مثل هذا النزاع لا يمكن أن يبرر في أية حالة رفض هذا الحامل رد عمليات الوفاء المنفذة من داينرز كلوب.

ثانيا- غياب التوقيع على فاتورة الشراء:

بعد إتمام عملية الشراء، وطباعة الفاتورة فقد ينسى التاجر أن يقوم بالحصول على توقيع الحامل على هذه الفاتورة، وبالتالي يثار نزاع فيما بعد بربط قيمة الفاتورة بالحامل، بالرغم من وجود بيانات البطاقة كافة على الفاتورة باستثناء توقيع الحامل، وفي حالة

منازعة الحامل على هذه الفاتورة غير الموقعة منه، فإن التاجر يجد نفسه في موقف صعب سبب عبء الإثبات الملقى على عاتقه، كذلك فإن المصدر غير ملزم بدفع الفاتورة غير الموقعة من الحامل[1].

اختلاف التوقيع على الفاتورة عن التوقيع المثبت على البطاقة: الأصل أن التوقيع المثبت على الفاتورة هو نفس توقيع الحامل المثبت لدى الجهة المصدرة وحتى يتحقق هذا الأخير من صحة الفاتورة فإن التوقيع على الفاتورة يجب أن يطابق نموذج توقيع الحامل المثبت لديه، كما يقع على التاجر التزام بأن يتحقق من أن التوقيع على الفاتورة يطابق التوقيع المثبت على البطاقة حتى لا يتعرض لمخاطر رفض الوفاء من قبل المصدر.

وقد قضت محكمة الاستئناف بباريس بقيام مسؤولية المصدر عن وفاء فواتير تحمل توقيعا مقلدا أو مختلفا عن نموذج توقيع الحامل المودع لديه، حتى وإن كانت الظروف لا تمكنه من القيام بهذا الفحص لتمام مقاصة الفواتير آليا.

ثالثا- عدم الحصول على تفويض من المؤسسة مصدرة بطاقة الدفع:

نصت جميع العقود المبرمة بين المصدر والتاجر على وجوب قيام التاجر بالحصول على تفويض أصلي من المؤسسة المالية رغم تنفيذ عملية الشراء بواسطة البطاقة مهما كان سقفها المحدد، ومهما كانت قيمة العملية وأن يقوم التاجر بأخذ رقم التفويض بعد الحصول عليه من المصدر وتثبيته في خانة مخصصة على الفاتورة، وفي حالة وقوع التاجر في هذا الخطأ فإنه يتحمل مخاطر عدم قيام المصدر بالوفاء بقيمة عملية الشراء التي قام بها الحامل[2].

---

[1]- فيعتبر التوقيع الأداة الوحيدة التي تربط هذه الفاتورة بالحامل، والتي تمثل مصدر الأمر بالوفاء، **أمجد حمدان الجهيني**، الاستخدامات غير مشروعة لبطاقات الدفع الالكتروني من قبل الغير، مركز الدراسات القضائية، مقال منشور في: www.coiss.com/replay.php، المملكة الأردنية الهاشمية، ص7، 2009/06/01.

[2]- يكون التفويض إلزامي في حالة الشراء بطريقة غير مباشرة Off-line أما في حالة الشراء بطريقة مباشرة On-line فلا حاجة للحصول على هذا التفويض حيث أن الجهاز الإلكتروني سوف يقوم برفض العملية الكترونيا في حالة عدم وجود رصيد أو كان الرصيد لا يغطي العملية المنفذة. أنظر: المرجع نفسه، ص8.

ولتمييز الاستخدام غير المشروع للبطاقة عن الأخطاء الفنية التي تحدث عند استخدامها يرى الدكتور أمجد حمدان الجهني، أن معيار التمييز بين الخطأ الفني والاستخدام غير المشروع هو في مدى توافر حسن أو سوء النية عند استخدام البطاقة، فإذا حدث عن حسن نية فيبقى هذا الاستخدام غير مشروع، وتقدير حسن النية أو سوء النية يعود إلى قاضي الموضوع وفق النزاع المطروح عليه[1].

المبحث الثاني

[1]- أنظر: **أمجد حمدان الجهيني**، الاستخدامات غير مشروعة لبطاقات الدفع الالكتروني من قبل الغير، مركز الدراسات القضائية، مقال منشور في: www.coiss.com/replay.php، المملكة الأردنية الهاشمية، ص6، 2009/06/01.

الحماية التقنية والقانونية لعملية الدفع الالكتروني

يعتبر مستقبل الدفع الالكتروني واعتماده من طرف المؤسسات المالية والمستهلكون مرهون بقدر الحماية التي تضمنها وتوفرها سواء من قبل المتعاملين بهذه التقنية، كمقدمي الخدمات على الخط والبنوك في مجال استعمال التكنولوجيات الحديثة للاتصالات التي تعتمد أساسا على برامج الحواسيب وقواعد البيانات مستعملة تشفير البيانات لحمايتها من السرقة.

ينتج عن هذه المخاطر خسارة الملايين من المعاملات عبر شبكات الاتصال وإنقاص الثقة في التعامل بهذه التقنية مما يعمل على تراجع التجارة الالكترونية وغيرها من الأعمال، فتصبح مهددة بالفشل بصورة كبيرة ما لم يرتفع مستوى الأمان والموثوقية الخاصتين بالإنترنت.

ومسألة حماية قواعد البيانات من أكثر المسائل أهمية وأولوية بالنسبة للمبرمج الإلكتروني وهناك وجهان رئيسيان لحماية قواعد البيانات. الأول متعلق بحقوق المبرمج والمتمثلة في حقوقه الفكرية والثاني متعلق بالعملاء المستخدمين للبرامج وكيفية منح الصلاحيات للمستخدمين[1].

وتماشيا مع التطور الهائل الذي شمل قطاع تقنية المعلومات على مختلف الأصعدة ومنها النشاط الاقتصادي خاصة وانفجار ثورة التكنولوجيا المصرفية والتي حققت نتائج إيجابية فيمكن تعريف أمن المعلومات أو البيانات "**بأنّها تأمين وصول البيانات المطلوبة دون زيادة أو نقصان وفي الصورة السليمة الصحيحة إلى المستفيد المعني بها دون غيره في الوقت الملائم دون تأخير**"[2].

خاصة بظهور وسائل الدفع الحديثة كالبطاقات البنكية (البلاستيكية) والتحويل الالكتروني للأموال وما يترتب عن ذلك من اختصار الوقت والجهد وتأمين سرعة التعامل

[1]- **أمجد جمالي**، حماية قواعد البيانات وصلاحيات المستخدمين، مقال منشور على العنوان: www.arabteam2000-Forum.com، مجلة الفريق العربي، 2 أفريل 2005، ص1.

[2] - **حابت أمال**، استغلال خدمات الانترنت، المرجع السابق، ص41

لذلك ولإنجاح وتوفير الضمان والثقة اللازمين اعتمدت الكثير من التقنيات والتي تعبر بنفسها برمجيات الحواسيب لتأمين هذه المعاملات وهذا ما سميناه بالحماية التقنية التي سندرسها (مطلب أول).

وإذا كانت مهمة حماية الدفع الالكتروني من مهام أصحاب الاختصاص في الإعلام الآلي والتقنيين لمعرفتهم بتلك المهارة وكيفية ردع الاعتداءات بمناسبة استعمال البيانات الالكترونية وانتقالها، فإنّهم ليسوا الوحيدين المعنيين بضرورة إرساء حماية، فالحماية التقنية لا تكفي وحدها إذا لم تكن مدعمة بحماية قانونية بسن مجموعة من النصوص التي تنظم معاملات الدفع الالكتروني بصفة خاصة والتجارة الالكترونية بصفة عامة.

ولإرساء هذه الحماية الضرورة ظهرت جهود على المستويين الداخلي والخارجي من أجل تحقيق تعاون دولي فعلي وفعال وذلك لتجاوز هذه المعاملات حدود الدولة الواحدة وبالتالي ضرورة تضافر الجهود من أجل تطوير هذه المعاملات من خلال اطمئنان المتعاملين في حالة معرفتهم بالحماية القانونية المضمونة لممارساتهم عبر شبكات الاتصالات.

الشيء الذي يدفع لتطور التجارة الالكترونية، لذلك ارتأينا دراسة الحماية القانونية التي تضمنها التشريعات الداخلية والجهود الدولية في هذا المجال (مطلب ثاني).

المطلب الأول

الحماية التقنية للدفع الالكتروني

تعتبر التجارة الالكترونية وليدة التطور التكنولوجي الهائل الذي عرف خاصة منذ خمسينات القرن الماضي. فكلما ظهرت تقنية جديدة إلاّ وحملت في طياتها مخاطرها وهو الشأن بالنسبة للدفع الالكتروني وقصد تأمينه ظهرت آليات تأخذ أشكالا مختلفة لسد الطرق في وجه القراصنة والسارقين على الخط بالاستيلاء عليها والاستعمال غير المشروع لها، وبالتالي سنتولى مفهوم الحماية التقنية (فرع أول).

إن الاهتمام بتطوير هذه الحماية بالقدر الذي يتماشى وأهمية التجارة الالكترونية دفع إلى ظهور تقنيات عديدة لحمايتها سواء التي يقوم بها المتعاملون كالتوقيع الالكتروني

أو التي توجد على شكل برامج الحواسب كالتشفير وبعض بروتوكولات الأمنية والتي نتطرق إليها (فرع ثاني).

الفرع الأول

مفهوم الحماية التقنية للدفع الالكتروني

تتعرض المؤسسات المتعاملة في التجارة الالكترونية لمخاطر الاعتداءات التقنية الناتجة عن التكنولوجيا الجديدة والأنظمة الجديدة التي تعتمد عليها كي تتم المعاملة بشكل مؤمن نظرا لتدخل قنوات الاتصال على الأنترنت والمفتوحة للجميع مما يعرض المعلومات الشخصية للخطر ومن أجل ردع هذه المخاطر ظهرت عدة تقنيات للتقليل منها والتي تسعى لضمانها المؤسسات للمستهلكين في الوقت الذي تتم فيه معاملة التجارة الالكترونية[1].

أولا- تعريف الحماية التقنية للدفع الالكتروني:

يعرفها الأستاذ محمد دباس الحميد «***أنّها حماية جميع أنواع المعلومات ومصادر الأدوات التي يتعامل معها وتعالجها من منظمة وغرفة تشغيل أجهزة، والأجهزة ووسائط التخزين والأفراد من السرقة والتزوير والتلف والضياع والاختراق***»[2].

كما يمكن تعريف أمن المعلومات بأنّه: «***حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة. ويتم ذلك عن طريق إتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات وهي الكنز الثمين الذي يجب على المنشأة المحافظة عليه***»[3].

---

[1]- **Jeffrey F Rayport, Bernard J. Jaurorski**, commerce électronique Traduit de l'américain par Francine Nézina Johanne champoux et Elisabéth Rochette, Edition Cheneliere/ McGram-Hill, Montréal – Toronto, 2003, P56.

[2]- **محمد دباس الحميد، ماركو ابراهيم نينو،** حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان-الأردن، 2007، ص34.

[3]- أمن المعلومات قضية ساخنة باستمرار وقد أثبتت أهميتها الفائقة في السنوات الأخيرة بالذات. فمنذ عشر سنوات فقط كنّا إذا أثرنا موضوع " الأمن" في مجال المعلومات أو الحاسبات كنّا نسمع منة يقول الأمن ليس مشكلة تبحث عن حل وإنما هو حلول تبحث عن مشكلة! ولكن هذه المقولة لم يعد لها وجود بعد التطور الكبير الذي شهدته التقنية في السنوات الأخيرة. أنظر: **حسن طاهر داود،** الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض، ص23.

كما يعتبر البعض هذه الحماية عبارة عن:

- المحافظة على إتاحة المعلومات وسلامتها وسريانها وملكيتها والاستفادة منها.
- هي الطرق والوسائل المعتمدة للتحكم في كافة أنواع مصادر المعلومات وحمايتها من السرقة والتشويه والابتزاز والتلاف والضياع والتزوير والاستخدام غير المرخص وغير القانوني.
- حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنظمة نفسها والأفراد العاملين فيها والأجهزة والحسابات ووسائط المعلومات التي تحتوي على بيانات المنظمة وذلك بإتباع إجراءات ووسائل عديدة تضمن في النهاية سلامة المعلومات.

ثانيا- طبيعة أمن المعلومات والبيانات:

فالاستعمال الهائل لشبكات الاتصال عن بعد والإنترنت خاصة أدى إلى إقحام كل المتعاملين في التجارة الالكترونية عامة وفي الدفع الالكتروني والتحويل الالكتروني للأموال خاصة إلى اهتمام الجميع بضرورة حماية هذه المعاملات.

1- من حيث المعنيين بتوفير أمن المعلومات:

أهمية قضية الأمن ازدادت في الآونة الأخيرة فأصبحت كما ذكرنا من قبل مشكلة تبحث عن حل. وأصبحت هذه القضية تهم رجال الأعمال والمتعاملين الاقتصاديين وكل من لديه أنظمة معلومات، وأصبحت تهم المستفيد العادي وتهم الشركات التي تقدم خدمات المعلومات وتهم مصممي النظم والتطبيقات، وكذلك الشركات المطورة للأجهزة والبرمجيات، بل هي تهم في الوقت نفسه رجال القانون والتشريع ورجال الأمن. وتهم متخصصي الاتصالات وتهم المدرسين والطلاب.

كما تهم مسئولي الرقابة سواء الرقابة المالية والرقابة الإدارية، وعلى رأسهم هؤلاء جميعا يأتي مسؤولوا أمن المعلومات كمهتمين رئيسيين بهذه القضية[1]. ويمكن القول أن قضية أمن المعلومات قضيتنا جميعا نظرا لأهمية البيانات والمعلومات في عصرنا الحالي.

---

[1]- **حسن طاهر داود،** الحاسب وأمن المعلومات، المرجع السابق، ص26.

وما يزيد الاهتمام بأمن المعلومات هو أنها تستخدم من قبل الجميع بلا استثناء: الدول، الشركات والأفراد. كما أنّها هدف للاختراق من جانب الكثير كذلك وأيضا بلا استثناء وتكون المعلومات في بعض الحالات الفاصل بين المكسب والخسارة للشركات ومن تم كيف نحمي هذه المعلومات من الأخطار التي تهددها[1].

ويمكننا القول في هذا الصدد أن الشركات (البنوك والتجار...) الذين يتعاملون بتقنية مؤمنة تبعث الثقة في المستهلكين بالتعامل معها على عكس الشركة التي لا توفر قدر معين من أمن المعاملات مما يجعل المتعاملين معها ينفرون من مجال تعاملها.

2- من حيث صناعة أمن المعلومات:

مشاكل أمن المعلومات تكمن على مستوى المستهلك أي المشتري أو الزبون، على مستوى العنوان الالكتروني للمؤسسة التجارية تتعامل عبر الإنترنت[2]، فتأمين المعلومات سمح بضمان من الناحية التكنولوجية المسار الجيد والصحيح للمعاملة التجارية وذلك بالضمان لأنظمة الحواسيب وتأمين تحويل البيانات ما بينها وذلك بالقدرة على:

- القدرة على الاستعمال (توفير هذه الخدمات، الموارد والبرامج اللائقة).
- عدم السماح بالدخول للمعطيات والموارد الرقمية سوى للأشخاص والبرامج ذات الاختصاص لضمان (السرية، صحة البيانات والمعطيات وكذلك الخدمات).
- التأكيد وتبيان أن المعاملة قد حدثت فعلاً (سيرورة المعاملة، دلائل وعدم الرجوع).
- تطبيق المعاملة وجعل الخدمات المرجوة في أوضاع جيدة والاستعمال اللائق (استمرارية الخدمات، أمن الاستعمالات وفعالية البرامج)[3].

فصناعة أمن المعلومات تتزايد تقنياتها ومجالاتها يوم بعد يوم وتزدحم الأسواق بمنتجاتها، فيوجد على سبيل المثال أكثر من خمسين شركة في العالم توفر برمجيات

1- المرجع نفسه، ص30.

2- **Solange Ghernaouti-Hélie**, Sécurité, Internet, stratégie et technologie, Édition Dunod, Paris, 2000, p229.

3 - **Solange Ghernaouti-Hélie**, Sécurité, Internet, stratégie et technologie, op.cit, p228.

جدران الحماية pare-feu وهذه مجرد تقنية واحدة من تقنيات أمن المعلومات وتؤكد المنافسة الحامية في الأسواق مدى اهتمام صناعة أمن المعلومات بمحاولة جذب انتباه العملاء خاصة أولئك الذين يتعاملون مع شبكات الأنترنت[1].

كما يوفر التطور التكنولوجي وصناعة أمن المعلومات الكثير من الحلول الخاصة بالدفع الالكتروني المؤمن على شبكة الإنترنت فيمكن إضافة مستويات متفاوتة من تأمين الدفع في الوقت نفسه وذلك من خلال التأكد:

- صحة الرقم المستعمل بما يتماشى مع نوع البطاقة المستعملة.
- صحة الرقم المقدم بما يتماشى مع بنك الحامل (أي البنك الذي يتعامل معه الحامل).
- قبول الدفع من خلال تجمعات البنوك، أو مؤسسة موثوق منها وبإضافة رقم المعاملة.

كما يمكن تطبيق مجموعة من الإجراءات للحد من مخاطر الاعتداءات المعلوماتية وخطر التزوير وذلك من خلال ما يلي:

- اختراع نظام أمن (Un label de sécurité) وذلك بتوحيد الأنظمة الموجودة.
- المراقبة والتأكيد الشديدين لهوية الأطراف المتدخلة في العملية، وضع نظام فعال للتأكد من هذه الأنظمة.
- إدماج أمن المحتويات الرقمية في السياسة الأمنية تماشيا مع التطورات والمستجدات التكنولوجية.
- تقوية حماية المستهلكين، بتحسيس المستعملين بالأخطار التي يمكن أن يواجهها مسار نقل المعلومات ما بين مراكز المعلومات والبنوك.
- التأكد من الدفع والطلب بالوسائل الخارجية عن شبكة الإنترنت كالهاتف مثلاً.

---

[1]- ومن ذا الذي لا يتعامل مع شبكة الإنترنت في عصرنا الحالي؟ أنظر: **حسن طاهر داود**، الحاسب وأمن المعلومات، المرجع السابق، ص ص30-31.

- استعمال إجراءات وتقنيات أمنية إضافية[1].

ثالثاً- الجهود الأوربية لحماية وتأمين الدفع الإلكتروني:

يعتبر تأمين معاملات الدفع الإلكتروني ذات أهمية بالغة وأولوية في مجال التجارة الإلكترونية، فمخاطر الدفع الإلكتروني تمس تقريبا 50% من المعاملات في فرنسا لذلك وضعت مجموعة من الإجراءات منها:

1. تعميم نظام (EMV)[2] وهو عبارة عن نموذج (Un standard) دولي للبطاقات الدولية الذي تم وضعه في سنة 1997 عن طريق شبكات دولية للدفع الدولي منها (Europay) ماستركارد وفيزا (Mastercard et Visa) لذا يعبر عنه باختصار (EMV). وهذا التقدم أو الاتحاد ما بين هذه المؤسسات يهدف إلى الاستجابة لما تنتظره البنوك في العالم، ويتمثل هدفها أولاً في تدعيم وتقوية استعمال البطاقات البنكية وذلك اعتمادا على تكنولوجيا الشفرة (La puce) التي تستوجب استعمال الرقم السري عند الدفع أو عند سحب النقود.

ومنذ استعمال الشفرة على البطاقات البنكية سنة 1992 سمح بتخفيض مخاطر الدفع بـ 10% ومن الناحية الأخرى فالنظام (EMV) يسمح بتوسيع نظام الخدمات المقدمة بواسطة البطاقات وذلك اعتمادا على قدرة الذكاء التي يتمتع بها والذاكرة (Microprocesseur) في مجالات عديدة منها تأمين خدمات البنوك عن بعد.

وذلك بتطويره عند استعمال هذه البطاقات مثل الموزعين الكترونيا لأوراق (les DAB) وles TPE (Terminaux de paiement électroniques) كذلك مراكز معالجة البنوك وتطويرها تماشيا مع المستجدات. وسعى هذا النظام إلى وضع كافة البطاقات البنكية المستعملة في أوربا بمعيار EMV كما يعتبر اعتماد هذا النظام من الناحية التنظيمية ثورة

1- Parmi les mesures de sécurité :
- Acceptation du paiement par le GIE Cartes Bancaires ou par un tiers organisme (avec le numéro de transaction).
- Utilisations des mesures de sécurité supplémentaires des «e-cartes bleus » (code à 3 chiffres ou dos de la carte) ». Voir : **Christophe Comborde**, sécurisez vos applications Internet (messagerie, Internet, site web, e-commerce), Éditions Dunod, Paris, 2004, p210.

2- **Regis Bouyala ,** le monde des paiements, op.cit, p 43.

حقيقية لكافة الدول الأوربية وغيرها، منها الولايات المتحدة الأمريكية والبرازيل اليابان والصين التي اهتمت بهذه المعايير[1].

رابعا-أهمية الحماية التقنية للمعلومات:

إن حماية الدفع الإلكتروني والبيانات عامة شيء بالغ الأهمية للبنوك ويترجم ذلك من خلال المبالغ المالية المستثمرة في هذا المجال من جهة كما تعتبر الأكثر عرضة للقرصنة، ويشكل الاعتداءات على الحسابات البنكية جريمة التحويل الإلكتروني غير المشروع للأموال الذي سنراه في دراستنا اللاحقة .

وعلى سبيل المثال فإن البنك BNP Paribas حسب تصريحات أحد مسؤوليه: ستقوم بتخصيص 2.8 مليار أورو، فالاستثمارات في أمن المعلوماتية في تطور مستمر وهذا تماشيا مع طبيعة المخاطر التي تهدد الأنظمة وبالتالي ضرورة جعلها آمنة واستغلالها لرفع من مداخل البنك.

ويستلزم ذلك وضع تحليل كلي لكل خطر وتطبيق قدرات البنك وذلك لحماية مصالح الزبائن وحماية سرية المعطيات والبيانات الشخصية، تطبيق التشريعات والتنظيمات وتنفيذها مثل السر المصرفي (Le secret bancaire) والأمن المالي، وحسب تصريحات المسؤول نفسه فالبنك ذاته ليس لديه مشكلة مع استعمال شبكة الإنترنت وذلك بمجرد التعرف على الزبون وقدراته العملية (Profil d’opération)، يستطيع التعرف على كل العمليات العادية وما الإنترنت إلاّ قناة للقيام بهذه العمليات وتوجد العديد من الوسائل والآليات لمحاربة التزوير عبر الإنترنت[2].

ولعل أهمية هذه المسألة تظهر كذلك من خلال الاهتمام الحريص الذي أولته لجنة الأمم المتحدة للقانون التجاري الدولي قانون الأنسيترال (UNICITRAL law) النموذجي الخاص بهذا الموضوع الذي يمكن الإشارة إليه وأخذه كأحد الأمثلة على التعاون الدولي على وضع إطار قانوني مشترك وفي الإطار نفسه نذكر المجهودات التي تقوم بها غرفة

---

1 - **Regis Bouyala ,** le monde des paiements, op.cit, p35.

2- **Gilles Mowas**, La sécurité des données dans les banques : enjeux et compétence, Éditions Jeudi mag, www.lesjeudis.com/magasineinformatique, publié le 24-09-2007, p.01.

التجارة الدولية ICC من أجل إنشاء قاعدة بيانات لمصطلحات التجارة الالكترونية والتي يمكن إدراجها في العقود التجارية المستخدمة في التجارة الالكترونية.

فالقانون النموذجي للتجارة الالكترونية(Électronique Commerce) قانون الأنسيترال يضع قواعد محددة بشأن التوقيعات الالكترونية، وإضافة لهذا فإن المقصود من إصدار هذا القانون النموذجي توفير إجراءات ومبادئ أساسية لتسهيل استخدام التقنيات الحديثة العصرية الخاصة بإدخال المعلومات (تدوينها) على الكمبيوتر أو نقلها أو إبلاغها إلى طرف ثان[1].

الفرع الثاني

الميكانيزمات التقنية لحماية الدفع الالكتروني

لقد دفع الطابع غير المادي للدفع الالكتروني إلى ضرورة إيجاد وسائل وتقنيات وضعت تحت تصرف المتعاملين بها كي يضمن أكبر قدر ممكن من الثقة والاطمئنان، من خلال استعمالها وكذلك إنجاح استعمالها وذلك بانتشارها في كافة المعاملات المالية والتجارية.

وبالتالي تستخدم العديد من التقنيات مثل التوقيع الالكتروني والرقمي وتشفير المعلومات والبيانات المرسلة على الخط (أولا) فلم تقف محاولات التأمين إلى هذا الحد بل توصلت إلى وضع برامج آمنة ينصح الزبائن باستعمالها وتسمى بالبروتوكولات المؤمنة **(ثانيا)**.

من بين الوسائل المخولة لمستعملي شبكة الأنترنت لتأمين معاملاتهم نجد مجموعة من التطبيقات التي يقوم بها مرسل أو مستعمل شبكات الاتصالات لتنفيذ عملية مالية بواسطة إلكترونية وتكمن في الرقم السري والتوقيع الالكتروني والرقمي.

[1]- ويجب القول أن هذا القانون النموذجي يعتبر قانونا مرجعيا أو استرشاديا ولا يشمل على كافة التفاصيل من الأحكام القانونية واللوائح التي تكون ضرورية لتطبيق هذه التقنيات. أنظر: **محمد الجنبيهي**، البنوك الالكترونية، المرجع السابق، ص ص82-83.

أولا- الرقم السري أو الكلمات السرية:

تعتبر الحماية بواسطة الرقم السري الإجراء المؤمن الأكثر استعمالا في المجال الرقمي في عصرنا الحالي، وإجراءات فتح النافذة واستعمال الرقم السري يسمح لصاحب البرامج التأكد من هوية المستعمل الذي يحاول الدخول إلى العنوان الالكتروني أو جزء منه، وذلك عند محاولته الدخول لنافذة مؤمنة، يجب استعماله لرقم سري لتأمين معاملاته، وعند تقديمه للرقم السري الصحيح يمكنه الدخول لما يريده من المعطيات والبيانات السرية والشخصية[1].

كما يعتبر استخدام كلمات المرور أرخص أسلوب كذلك ولكي يحقق هذا الأسلوب النجاح يجب توعية المستخدمين بعدم التخلي عن كلمة المرور لأي شخص، وأن يفرض عليهم تغييرها بصفة دورية ويجب كذلك تشفير كلمات المرور في الملفات المستخدمة لحفظها في الحاسب وعند إدخال كلمة المرور لا يجب أن يظهر النظام حروفها حتى لا تنكشف أمام المتطفلين.

كما تتبع بعض الجهات أسلوب تخصيص كلمات المرور بواسطة الشبكة أو مسؤول أمن النظام، وذلك للحد من المحاولات البسيطة لتخمين كلمة المرور والتي قد تكون اسم أحد أبناء المستخدم أو تاريخ ميلاده مثلا.

ومن عيوب هذا الأسلوب أنه يمكن كسره بسهولة بواسطة برامج تقوم بجعل عدد لا نهائي من المحاولات حتى تتوصل إلى الكلمة الصحيحة وبذلك تحديد عدد المحاولات الفاشلة التي يتم بعدها فصل الطرفية واتفاقها عن العمل تماما[2]، كما طرح المصرف التجاري السوري عددا من المميزات الخاصة ببطاقة الدفع الالكتروني وأصبح بإمكان

---

[1] - **Jeffrey F Rayport, Bernard J. Jaurorski**, commerce électronique, op-cit, p. 56.

[2] - **حسن طاهر داود،** الحاسب وأمن المعلومات، المرجع السابق، ص ص310-311.

- Il s’agit de garder secrets leurs mots de passe, certains utilisateur en font part à des amis, les écrivent à des endroits ou ils peuvent être découverts ou choisissent un mot de passe facile à deviner. Voir : **Jeffrey F Rayport, Bernard J. Jaurorski**, commerce électronique, op-cit, p.57.

المتعامل صاحب البطاقة الالكترونية تغيير الرقم السري من خلال الصراف الآلي نفسه دون أن تكون هناك حاجة لمراجعة أي فرع من فروع المصرف[1].

ثانيا- التوقيع الالكتروني كآلية لحماية البيانات:

التوقيع الالكتروني عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام والرموز الالكترونية تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا ويطلق عليها اسم الشهادة الرقمية (Certification électronique).

وتخزن في هذا الملف جميع معلومات الشخص وتاريخ ورقم الشهادة ومصدرها وعادة يسلم مع هذه الشهادة مفتاحان أحدهما عام والأخر خاص، أما المفتاح العام فهو الذي ينشر في الدليل لكل الناس والمفتاح الخاص هو توقيعك الالكتروني وتقوم الهيئات بإصدار تلك الشهادات الرقمية والتي تكون مقابل رسوم معينة.

وباختصار شديد يمكن تعريف التوقيع الالكتروني أنّه «طريقة اتصال مشفرة رقميا تعمل على توثيق المعاملات بشتى أنواعها والتي تتم عبر صفحات الإنترنت».

كما عرفته المادة 2 من قانون توقيع الكتروني الأنسيترال النموذجي بشأن التوقيعات الإلكترونية الصادر سنة2001 في فقرتها "أ" أنّه «***يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها ومرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموّقع على المعلومات الواردة في رسالة البيانات***»[2].

وهناك مقاربات أخرى فيرى البعض أنه عبارة عن حروف أو أرقام أو رموز أو إشارات تأخذ شكل إلكتروني لها طابعا منفردا يسمح بتحديد الشخص صاحب التوقيع وتمييزه عن غيره. كما عرفته المادة 1/2 من التوجيه الأوربي رقم 93/1999 بأنه

---

[1]- المصرف التجاري يطلق مميزات جديدة على بطاقة الدفع الالكتروني، مقال منشور على المقال الالكتروني www.banquecentral.gov.sy/archive.

[2]- أنظر : في ذلك نص المادة 1/2 من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية الصادرة عن لجنة الأمم المتحدة للقانون التجاري الدولي الصادر في 05 جويلية2001.

المعطيات التي تأخذ الشكل الإلكتروني والتي ترتبط بمعطيات أخرى إلكترونية والتي تستخدم كوسيلة لإثبات صحتها[1].

1- أنواع التوقيعات الالكترونية:

أ- التوقيع المحمي: وهنا يتم تزويد الوثيقة الالكترونية بتوقيع رقمي مشفرة تقوم بتشخيص المستخدم "الموقع" الذي قام بالتوقيع ووقت التوقيع ومعلومات الشخص نفسه وهو عادة مميز لأصحاب التوقيع.

ب- التوقيع البيومتري: يقوم الموقع هنا باستخدام قلم إلكتروني يتم توصيله بجهاز الكمبيوتر ويبدأ الشخص بالتوقيع باستخدام القلم مما يسجل نمط حركات يد الشخص وأصابعه، ولكل منّا نمط مختلف عن الآخر حيث يتم تحديد هذه السمة وهنا تقودنا أيضا إلى البصمة الإلكترونية التي تعمل بنفس التقنية .

2- الهدف من التوقيع الالكتروني:

يندرج الهدف تحت مضمون الأمن والسلامة الرقميين، وعند ثبوت صحتها فإنها بالطبع تحقق جميع الجوانب العملية والأهداف المرجوة منها ولعدة أهداف قانونية بحتة تبعد المتطفلين عن التلصص وسرقة البيانات[2]. وتكمن الموثوقية التي يتمتع بها هذا النوع من التوقيع في مدى صحته وتكون هذا التحقيق بإحدى الطريقتين:

- عن طريق سلطات التوثيق التي تقوم بمنح شهادة رقمية لذوي الشأن تؤكد حجية إرسال الرسالة حيث يتم تخزين هذه الشهادة على الكمبيوتر (on-line) ويمكن أن يصل إلى الجميع للتحقق من مطابقتها للأصل عبر التوقيع الرقمي للسلطة حيث يمكن التثبت منها بالمفتاح العام الخاص بالشهادة.

---

[1]- والمشكل في هذه التعاريف هو ورود لفظ "الشكل الإلكتروني"، فليس باستطاعة الكافة التمييز بين ما هو إلكتروني وما هو غير ذلك، كالشكل الكهربائي أو بالأشعة أنظر: **حابت أمال، استغلال خدمات الانترنت**، المرجع السابق، ص86.

[2]- **أسامة الكسواني**، التوقيع الإلكتروني، المجلة الإلكترونية، مقال منشور على الموقع الالكتروني: http://news.maktoub.com/article، ص3.

- عن طريق قيام مستلم الرسالة بتشفير جزء من الرسالة باستخدام المفتاح العام المرسل وبرنامج التشفير المستخدم في تشفير الرسالة فإذا كانت النتيجة واحدة فهذا يدل على صحة الرسالة والتوثق من المرسل[1].

كما أولت لجنة الأمم المتحدة للتجارة الدولية اهتماما بالغا بالتوقيع الإلكتروني بإدراجه في القانون النموذجي، ويظهر ذلك من نص المادة العاشرة المعنونة بالجدارة بالثقة والتي تنص: "لأغراض الفقرة 1 (و) من المادة 09 من هذا القانون، يجوز لدى تقرير ما إذا كانت أي نظم وإجراءات وموارد بشرية يستخدمها مقدم خدمات التصديق جديرة بالثقة أو لدى تقرير جدارتها بالثقة إيلاء الاعتبار للعوامل التالية:

أ. «الموارد المالية والبشرية، بما في ذلك توافر الموجودات.

ب. جودة نوعية نظم المعدات والبرمجيات.

ج. إجراءات تجهيز الشهادات وطلبات الحصول على الشهادات والاحتفاظ بالسجلات.

د. إتاحة المعلومات للموقّعين المعينة هويتهم في الشهادات وللأطراف المعولة المحتملة.

ه. انتظام ومدى مراجعة الحسابات من جانب هيئة مستقلة.

و. وجود إعلان من الدولة أو من هيئة اعتماد أو من مقدم خدمات التصديق بخصوص الامتثال لما سبق ذكره أو بخصوص وجوده.

ز. أي عامل آخر ذي صلة»[2].

1- **نضال إسماعيل برهم**، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2005، عمان، ص ص174-175. أنظر كذلك: يجب التحقق من أمرين، التحقق من صلاحية الشهادة أو وقفها أو إلغائها ومراعاة وجود أي تغيير بخصوص الشهادة. ونعني بالشهادة رسالة بيانات أو سجلا آخر يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع، **وائل أنور بندق**، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، المرجع السابق، ص ص103-107.

2- أنظر: في ذلك نص المادة 10 من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية الصادرة عن لجنة الأمم المتحدة للقانون التجاري الدولي الصادر في 05 جويلية2001.

3- الاعتراف القانوني الداخلي بالتوقيع الإلكتروني: كان أول اعتراف بالتوقيع الإلكتروني في عام 1989 في مجال البطاقات الائتمانية حيث أقرت محكمة النقض الفرنسية صحة التوقيع الإلكتروني واعتبرته يتألف من عنصرين هما: إبراز البطاقة الائتمانية وإدخال رقم حامل البطاقة السري وأكدت هذه المحكمة كذلك أن هذه الوسيلة توفر الضمان الموجودة في التوقيع اليدوي بل تفوقها.

وفي 13 آذار 2000 صدر في فرنسا تعديل على قانون الإثبات أضفى بعدا جديدا للإثبات الخطي حيث استوعب المستند الإلكتروني كما أعطى تعريفا واسعا للتوقيع مركزا على وظيفة التوقيع وغايته وليس على شكله، حيث استبعدت المادة 4/1316 عبارة التوقيع بخط يده واستبدلتها بعبارة التوقيع الصادر منه بدون أي تحديد لشكلية التوقيع.

كما جاء في نص المادة 06 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية (2001) أنّه:

1. حيثما يشترط القانون وجود توقيع من شخص، يعد ذلك الاشتراط مستوفي بالنسبة إلى رسالة البيانات إذا استخدم توقيع الكتروني يعول عليه بالقدر المناسب للغرض الذي أنشأت أو أبلغت من أجله رسالة البيانات في ضوء كل ظروف بما في ذلك أي اتفاق ذي صلة.

2. تطبق الفقرة الأولى سواء كان الاشتراط المشار إليه فيها في شكل التزام أم كان القانون يكتفي بالنص على التبعات تترتب عدم وجود توقيع.

3. يعتبر التوقيع الالكتروني قابلا للتعويل عليه لغرض الوفاء للاشتراط المشار إليه في الفقرة 1 إذا:

أ. كانت بيانات إنشاء التوقيع مرتبط في السياق الذي تستخدم فيه بالموقّع دون أي شخص آخر.

ب.كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع للسيطرة الموقع دون شخص آخر.

ج. كان أي تغيير في التوقيع الالكتروني يجرى بعد حدوث التوقيع قابلا للاكتشاف.

د. كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجرى في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف(1).

وتظهر حجية التوقيع الإلكتروني بمختلف أشكاله في الاعتراف القانوني لها، وكان هذا الهدف أساسي لتوصية الاتحاد الأوربي الخاصة بالتوقيع الإلكتروني لسنـة 2000 وهذا الهدف هو الذي سمح بترقية التجارة الإلكترونية إذا اعترف بالقيمة القانونية للتوقيع الإلكتروني في مختلف الدول الأعضاء، كما يظهر ذلك من خلال آثار التوقيع الإلكتروني. فعلى الدول الأعضاء:

- السهر والعمل على إتمام التوقيع الإلكتروني السالف تعريف أن يتم بوسائل مؤمنة وملائمة للقيام بالتوقيع الإلكتروني.

- الاستجابة للمتطلبات الشرعية للتوقيع بالمعطيات الإلكترونية بنفس حجية التوقيع اليدوي التقليدي.

- الاعتراف بالتوقيع الإلكتروني بصفته إشهادا قانونيا (Preuve de justice)(2).

وحسب تقديرنا فإن الجهود الدولية والإقليمية التي بذلت في هذا المقام غرضها التشجيع على اعتماد هذه القواعد النموذجية وترسيخها في القوانين الداخلية للدول.

1- **نضال إسماعيل برهم**، أحكام عقود التجارة الإلكترونية، المرجع السابق، ص177-178. أنظر كذلك:

يشترط في التوقيع أن يكون مطابقا، أي يتم وفقا للأسلوب الذي درج الشخص على استخدامه للتعبير عن قبوله محرر معين ورضائه بمضمونه، بحيث يكون التوقيع دالا على شخصية صاحبه، ومميزا لهوية الموقع وتعبيرا عن رضائه الالتزام بمضمون المحرر.

فالتوقيع الالكتروني على عكس التوقيع في الشكل الكتابي لا يقتصر على الإمضاء أو بصمة الأصابع، بل يشمل صورا لا تقع تحت حصر منها: صور أو حروف أو أرقام أو رموز أو إشارات أو حتى أصوات بشرط أن يكون لها طابع فردي. كما يتميز بأنه لا يتم عبر وسيط مادي وإنما يتم كليا أو جزئيا عبر وسيط الكتروني من خلال الحاسب الآلي، **محمد بودالي**، التوقيع الالكتروني، مجلة المدرسة الوطنية للإدارة(إدارة)، العدد 26، 2003، ص53-57.

2 - **Mireille Antoine**, La directive européenne sur la signature électronique : vers la sécurisation des transactions sur Internet ? www.droit-technologie.org, 5-10-2000, p 2 et 5.

أ- في القانون الفرنسي: ففي 21 جوان 2004 اعتمد المشرع الفرنسي القانون رقم 75-2004 الخاص بالثقة في الاقتصاد الرقمي (LCEN) الذي جاء لتكميل النظام التشريعي المعتمد عن طريق قانون 13 مارس 2000 الذي ينص أن الكتابة لازمة لصحة العقد. فأوسع القانون 75-2004 الاعتراف بالمحرر الإلكتروني ويظهر ذلك من خلال المادة 1108-1 من القانون المدني الفرنسي والتي تنص: "عندما يستلزم محرر كتابي لصحة عمل قانوني، يمكن أن يستحدث ويحفظ بطريقة إلكترونية"[(1)].

ب- في التشريع الألماني: تدخل المشرع الألماني بقانون 15 ماي 1986 والذي عدل بمقتضاه قانون العقوبات بأن أضاف إليه المادة 202 (أ) والتي جرم فيها فعل التجسس على المعلومات المخزنة. وقد وردت هذه المادة في الباب الخاص بجرائم الاعتداء على الحياة الخاصة والسر اللذين جمعهما المشرع الألماني في باب واحد، ولعلّه ذلك الارتباط الوثيق بين فكرة السر والحياة الخاصة وأن عناصرها تتحدد في حماية سرية المحادثات وحماية سرية المراسلات وحماية الأسرار الخاصة لأفراد.

كما أصدر المشرع الألماني قانون للتوقيع الالكتروني دخل حيز النفاذ في 1 نوفمبر 1997، وقد نص المشرع الألماني في هذا القانون على القواعد التوقيع الالكتروني مثل تعريف الاصطلاحات الواردة في التشريع وتحديد السلطة المختصة بتطبيقه، والقواعد المتعلقة بمقدمي خدمة التوثيق وسلامة الفنية، كما نص كذلك على القواعد الخاصة من المسؤولية والجزاءات الموقعة، كما اصدر المشرع الألماني قانون المعلومات وخدمات الاتصال والذي دخل حيز النفاذ في 01 أوت 1997[(2)].

ج- في القانون الجزائري: نصت المادة 323 مكرر 1من القانون المدني التي أضيفت بموجب القانون رقم05-01 المؤرخ في 20 يونيو 2005 على: "يعتبر الإثبات

---

[1]- Article 1108-1 du Code civil français : « Lorsqu'un écrit exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique », in : Olive Leclerc, La reconnaissance de la signature électronique : **Caroline Riet,** Étude comparée des législations françaises et allemande, http://m2bde.u-paris10.fr, 23 juin 2008, p5.

[2]- **اشرف توفيق شمس دين،** الحماية الجنائية للمستند الالكتروني، دراسة مقارنة، دراسة مقدمة في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، مركز البحوث والدراسات من 26 نيسيان إلى 28 نيسيان 2003، دبي، منشور على الموقع: http://www.lawjo.net

بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق..."[1]. كما تجدر الإشارة إلى اتجاه الدولة إلى ترسيخ الوثائق البيوميترية للهوية مثل جواز السفر يعد من قبيل توسيع الاعتراف وتوسيع استعمال التوقيع الإلكتروني. كما نصت المادة الثالثة فقرة 2 من المرسوم التنفيذي 07-162 على: التوقيع الالكتروني المؤمن يفي بالمتطلبات الآتية:

- يكون خاص بالموقع.
- يتم إنشاءه بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصرية.
- يضمن مع الفعل المرتبط به،صلة حيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه[2].

ثالثا-الاعتراف بالتوقيعات الالكترونية الأجنبية:

نصت المادة الثالثة مكرر1 من المرسوم التنفيذي 07-162 السالف ذكره على: "تكون للشهادات التي يسلمها مؤدي خدمات تصديق الكتروني مقيم في بلد أجنبي، نفس قيمة الشهادة المسلمة بموجب أحكام هذا المرسوم إذا كان هذا المؤدي الأجنبي يتصرف في إطار اتفاقية للاعتراف المتبادل أبرمتها سلطة ضبط البريد والمواصلات السلكية واللاسلكية"[(3)]، فيعتبر اعتراف صريح بالتوقيعات الأجنبية، بشرط أن يكون التصرف القانوني في إطار اتفاقية للاعتراف المتبادل بحجية التوقيع الالكتروني بين أطراف الاتفاقية.

ويأخذ بعين الاعتبار بصفة عامة لدى تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني ساري المفعول قانونيا أو مدى كونهما كذلك، لا يولى أي اعتبار لما يلي:

---

[1]- المادة 323 مكرر 1 من القانون المدني الجزائري.

[2]- كما نص القانون في المادة نفسها على معطيات وأجهزة فحص التوقيع الالكتروني راجع: المرسوم التنفيذي رقم 07-162 المؤرخ في 13 جمادي الأولى عام 1428 الموافق 30 مايو سنة 2007.يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 15 صفر عام 1422 الموافق 9 مايو سنة 2001، والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية. ج.ر العدد37، 2007.

[3]- راجع المادة الثالثة مكرر1 من المرسوم 07-162 السالف الإشارة إليه.

- الموقع الجغرافي الذي تصدر فيه الشهادة أو ينشأ أو يستخدم فيه التوقيع الإلكتروني.
- الموقع الجغرافي لمكان علم المصدر أو الموقع.
- يكون للتوقيع الإلكتروني الذي ينشأ أو يستخدم خارج الدولة المشرعة المفعول القانوني نفسه في الدولة المشرعة الذي للتوقيع الإلكتروني الذي ينشئه أو يستخدمه في الدولة المشرعة، إذا كان يتيح مستوى متكافئا جوهريا من الموثوقية.
- لدى تقرير ما إذا الشهادة أو التوقيع الإلكتروني يتيحان مستوى متكافئا جوهريا من الموثوقية، يولي الاعتبار للمعايير الدولية المعترف بها ولأي عوامل أخرى ذات صلة.
- إذا اتفقت الأطراف فيما بينها على استخدام أنواع معينة من التوقيعات الإلكترونية أو الشهادات، يتعين الاعتراف بذلك الاتفاق باعتباره كافيا لأغراض الاعتراف عبر الحدود ما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضى القانون المطبق[1]. وهذا ما نصت عليه المادة 12 من قانون الأنسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001.

رابعا- تشفير البيانات كوسيلة لتأمين الدفع الإلكتروني:

ومن بين التقنية التي استعملت في هذا المجال لتأمين عمليات مؤمنة من كل اختراق أو اعتداء عليها، تستعمل عملية التشفير كآلية لتحقيق ذات الهدف.

1-تعريف التشفير:

هو ما يطلق عليها أيضا لفظ "**التعميه**" للتعبير عن الرسالة المشفرة بحيث لو تم اعتراض الرسالة فلا ينكشف مضمونها. هذا باختصار هو التشفير (Encrypt) وهو وسيلة للحفاظ على أمن المعلومات من نية غير آمنة.

---

[1]- **وائل أنور بندق**، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، المرجع السابق، ص108-109.

ويقول الأستاذ "بوير" أن أكثر وسائل أمن المعلومات فعالية هي التشفير يعرفه على النحو التالي: "تشفير المعلومات هو تغيير مظهرها بحيث يختفي مظهرها الحقيقي بحيث تكون غير مفهومة لمن يتلصص عليها. يستطيع أخصائيو أمن المعلومات منع الأشخاص غير المرخص لهم من الاطلاع على هذه البيانات وبذلك يحقق التشفير سرية البيانات[1] كتشفير أرقام بطاقات الدفع أو غيرها من البيانات.

كما يعرفه البعض على أنها تكنولوجيا تستعمل خورزميات رياضية معقدة لتشفير ونزع تشفير البيانات وهذا بهدف ضمان السرية التي تستلزمها المعلومات بقصد تأمين المعاملات ما بين الزبون على الخط والتاجر أو البنك بقصد أن تنحصر قراءتها والإطلاع عليها على المعنيين الشرعيين لهذه العملية[2].

وتقوم عادة الكثير من المواقع العالمية بعدة إجراءات احترازية بخلاف ما تتخذه من ترتيبات متعلقة بتكنولوجيا الحماية فتتخذ الإجراءات العديدة التالية:

- حصر فتح المعلومات المشفرة على عدد قليل من الموظفين الموثوق بهم.

- يتم توزيع المعلومات بعد فتحها وفرزها إلى الأقسام المتخصصة إلكترونيا بحيث لا يتم إعطاء أي قسم سوى المعلومات التي يحتاجها فعليا، فمثلاً لا يتم إعطاء رقم بطاقة الدفع إلى قسم المحاسبة لخصم المبلغ ويتم تشفيرها مرة أخرى ولا يمكن لأي شخص أن يطلع عليها.

- يقوم الموقع بإضافة جميع البيانات الخاصة بالزبائن في بنك المعلومات الخاصة به وهو محمي بجدران النار وكلمات المرور ولا يمكن لأي شخص غير مخول له بالوصول إليها.

- تقوم المواقع بعمل عدة طبقات من الصلاحيات للموظفين بحيث لا يمكن لأي موظف الوصول إلى معلومات غير مسموح له بالوصول إليها، فمثلا موظف في قسم

---

[1]- **حسن طاهر داود**، الحاسب وأمن المعلومات، المرجع السابق، ص176.

[2]- **Jeffrey F Rayport, Bernard J. Jaurorski**, commerce électronique, op.cit, p57. Voir aussi : Caroline BOISSEL, E-Greffe, de la dématérialisation des actes de procédures vers le développement d'une justice en ligne ? D.E.SS Droit et Pratique du commerce électronique, Université Paris V, Paris, 2004 in www.droit.univ-paris5.fr

الشحن ليست له صلاحيات غير الوصول إلى معلومات محددة مثل طبيعة السلعة ورقم الطلبية وتاريخها وعنوان المرسل إليه[1].

كما يعرف التشفير بأنه عملية تحويل المعلومات إلى شفرات غير مفهومة (حتى تبدو غير ذات المعنى) لمنع الأشخاص غير المرخص لهم بالإطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة وتستخدم مفاتيح معينة في تشفير الرسالة وفك تشفيرها. وتستند هذه المفاتيح إلى صيغ رياضية وخوارزميات معقدة، وتعتمد قوة وفعالية التشفير على عاملين أساسيين: الخوارزمية وطول المفتاح رقميا[2].

ويمكن تعريف التشفير أيضا أنّه علم يستعمل الوسائل والتقنيات لتغيير طبيعة البيانات باستعمال الرياضيات لتشفير وفك تشفير البيانات. وبالتالي يسمح بتخزين المعلومات السرية أو إرسالها على قنوات غير مؤمنة مثل الإنترنت بهدف عدم قراءتها من أي شخص آخر وعدم تغييرها للاستعمال غير المشروع بعد الاعتداء عليها[3].

2- آلية استخدام التشفير:

يستلزم استخدام تشفير المعلومات تركيب برامج مخصصة لذلك على حاسوب كل من المرسل ومتلقي المعلومة أو البيانات، فبعد كتابة الرقم السري للبطاقة أو رقم الحساب مثلا يستعمل البرنامج المخصص للتشفير لتشفير هذه الأرقام قبل بعثها إلى التاجر أو البنك، فيتلقى التاجر أو البنك هذه الرسالة مشفرة فيستعمل بدوره البرنامج المخصص لفك

1- **إبراهيم بختي**، التجارة الإلكترونية، مفاهيم واستراتيجيات التطبيق في المؤسسة، ديوان المطبوعات الجامعية، الجزائر، 2005، ص81.

2- المرجع نفسه، ص77-78.

3-La cryptographie est la discipline incluant les principes, les moyens, et les méthodes de transformation des données dans le but de masqué un contenu, empêcher leur modification ou leur utilisation illégale.
Un moyen de cryptologie est défini comme tout matériel ou logiciel conçu pour transformé des données, qu'il s'agisse d'information ou de signaux, ces moyens ont principalement pour objet de garantir la sécurité du stockage ou de la transmission des données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité: **Sophia binet**, l'utilisation des nouvelles technologies dans le procès civil, vers une procédure civile intégralement informatisée? Mémoire master droit processuel, Université lumière Lyon 2, p45, In : www.mémoireonline.com

التشفير ليتمكن من قراءته، وإذا تمكن شخص بطريقة أو بأخرى الحصول على نسخة من الرسالة فلا يمكنه قراءتها لأنها مشفرة.

3- مفاتيح فك التشفير:

يجب أن نتساءل عن حالة ما إذا تمكن شخص أجنبي عن العلاقة من الحصول على الرسالة المشفرة فهل يمكنه استعمال أي برنامج لفك التشفير للرسالة الملتقطة؟ فهذا لا يمكن حدوثه فبرنامج فك التشفير يستعمل وسائل إضافية والمتمثلة في مفاتيح لغرض حصر قراءة الرسالة بين المرسل والمرسل إليه.

فعادة يكون مفتاحان: مفتاح عام ومفتاح خاص، فهذا شيء ضروري لإرسال المعلومة من حاسوب لآخر.

فالمفتاح العام يستعمل لغرض تشفير المعلومات المرسلة إلى الحاسوب الذي يملك صاحبه مفتاح خاص يتماشى مع المفتاح العام، فيستعمل المفتاح الخاص لفك تشفير البيانات التي تلقاها من الحاسوب الذي يملك مفتاح عام. فيعتمد هذا البروتوكول على خوارزميات المفتاح العام والمفتاح الخاص، ويقوم البنك أو المؤسسة بتزويد الزبائن بالمفاتيح العامة وتستخدم هذه المفاتيح العامة في تشفير الرسائل المتجهة إلى المؤسسة ولا يمكن استخدام المفتاح العام لفك شفرة الرسالة التي شفرها، إذ ينفرد المفتاح الخاص لدى المؤسسة بالقدرة على فك شفرة الرسالة التي شفرها المفتاح العام[1].

4- أهمية التشفير لتأمين البيانات:

عن طريق هذه التقنية يمكننا التغلب وتجاوز الكثير من المخاطر، فبواسطتها نتجنب:

- الإطلاع على المعلومات المحظورة (السرية) والشخصية.
- محاولة تعديل البيانات المنقولة بالشبكة.

---

[1]- **Jeffrey F Rayport, Bernard J. Jaurorski**, commerce électronique, op.cit, p.58.voir aussi :
-Sécuriser une transaction bancaire ne peut plus seulement vouloir dire crypter des données entre un internaute client et un site marchand ou une banque à l'aide du protocole SSL, ce que tous les prestataires de paiement se limitent a faire aujourd'hui la plus part du temps, mais aussi et surtout pouvoir contrôler, certifier et garantir a la fois que l'internaute agis bien avec l'accord du porteur, et surtout qu'il ne va pas ensuite s'opposer au paiement, une fois le bien matériel ou immatériel livré : **Olivier Rimmel**, en 2004 la fraude a la carte bancaire sur internet augmente toujours en Europe, 7 février 2005. In: http://epaysecurity.com

- إعادة توجيه البيانات إلى وجهة أخرى.
- تغيير محتويات الرسائل المتبادلة.
- تغيير كلمات السر الخاصة بالمستفيدين.
- انتحال شخصية المستخدم الحقيقي.
- تعديل الحسابات المخزنة على الحسابات نفسها[1].

ومن بين أنظمة التشفير الأكثر استعمالا نذكر نظام SSL والذي يعتبر اختصار لـ (Secure Sockets Layer) (SSL) يعتبر بروتوكول الطبقات الآمنة فيقوم بتأمين المعلومات بين المقدم والزبون، حيث يتم تشفير بيانات الرسالة المرسلة من المشتري إلى البائع ويتم إرسالها عبر الإنترنت أو البريد الإلكتروني.

فلا يتمكن لقراصنة الإنترنت من التقاط أرقام البطاقات البنكية، ولا تزوير المحررات الإلكترونية فيتم تشفير البيانات التي تتداول بين الحواسيب عبر برامج تصفح بيانات (المشتري) وبين مقر المعلومات الذي يتصفحه البائع[2]. فهذا النظام يندمج داخل قناة الاتصالات الإلكترونية بطريقة التي تسمح له بضمان شفاف لمستعمل تشفير المعطيات بهدف ضمان السرية.

ويضمن نظام (SSL) مستوى كاف للإرسال الآمن مثلا المراسلات الخاصة برقم بطاقة الدفع على الخط ولا يجب تأمين المعلومات فقط حين إرسالها على الخط وإنّما ضمان هذه الحماية طول مدة صلاحية المعلومة[3].

ويستخدم مع تكنولوجيا التشفير نظام الشهادات الموثقة الذي ينفذه طرف ثالث لتأكيد أن العميل الحقيقي هو الذي يتعامل مع الموقع وبذلك يتم من خلال الجمع بين هاتين

---

[1]- كما توجد أساليب كثيرة لتشفير البيانات مثل، شفرة قيصر (المفتاح السري)، نظام تشفير البيانات القياسي (Data encryption standard) أو DES، نظام RSA للتشفير (Rivest, Shamin et Adleman). راجع: **حسن طاهر داود**، الحاسب وأمن المعلومات، المرجع السابق، ص178-179.

[2]- **نادر شعبان إبراهيم السواح**، النقود البلاستيكية واثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، الدار الجامعية، 2006، ص124.

[3]- **Solange Ghernaouti-Hélie**, Sécurité Internet, Stratégie et technologie, Éditions Dunod, 2000, Paris, pp.129-130.

الوسيلتين ضمان سرية المعاملات التجارية وعقد صفقات آمنة، فحينما تقوم إحدى الشركات بإنشاء موقع لها باستخدام جهاز خدمة آمن (Secure Server) يتفق الحاسوبان على رموز حسابية شفرية ومفاتيح تشفير خاصة يستخدم تقنية تأمين المعلومات في تفكيكها وإعادة جمعها ويزود كل مستخدم أو عميل بمفتاحين للتشفير أحدهما خاص والآخر عام[1] كما ذكرنا سالفا.

الفرع الثالث

نماذج من برامج تأمين البيانات

لقد دفع مؤيدو تطوير التجارة الإلكترونية بصفة عامة والدفع الإلكتروني بصفة خاصة إلى الوضع العديد من برامج أمن مراسلات التجارة الإلكترونية وذلك بهدف ضمان الثقة في هذه المعاملات مما يساعد على تطويرها وترقيتها.

أولا- بروتوكول الحركات المالية الآمنة SET (Secure Electronic transaction):

يعتبر من أهم بروتوكولات أمن المعاملات الإلكترونية لتحقيقه غاية ضمان الحفاظ على أمن البيانات (خصوصيتها وسلامتها والتحقق من وصولها إلى الجهة المطلوبة) أثناء إجراء الحركات المالية عبر شبكة مفتوحة مثل الإنترنت. يستخدم هذا البروتوكول برمجيات تدعى "برمجيات المحفظة الإلكترونية".

وتحتوي هذه الأخيرة على رقم حامل البطاقة والشهادة الرقمية التابعة له أما التاجر فتكون له شهادة رقمية صادرة عن إحدى البنوك المعتمدة. ويستخدم كل من حامل البطاقة والتاجر الشهادة الرقمية التابعة له مما يتيح لكل منهما التحقق من هوية الآخر عند إجراء الحركات المالية عبر الإنترنت.

ولا يمكن للتاجر مشاهدة رقم البطاقة الائتمانية أثناء استعمال بروتوكول الحركات المالية الآمنة، حيث ترسل الصيغة المشفرة لهذا الرقم إلى مصدر هذه البطاقة للموافقة

[1] - **نضال إسماعيل برهم**، أحكام عقود التجارة الالكترونية، المرجع السابق، ص129.

على إجراء الحركة المالية مع التاجر، وتضمن هذه الطريقة عدم عرض الرقم، كما تمنع أي تعديل غير مرخص به أثناء إرسال البيانات[1].

ففي عام 1996 صدر النظام الجديد المشترك للمعاملات الإلكترونية الآمنة بعد التعاون بين أكبر مؤسسات لإصدار بطاقات البنكية في العالم وهم مؤسسة "الفيزا" و"ماستركارد" وأيضا انضمت إليها "أمريكان إكسبرس". ويعتمد هذا النظام (**SET**) على قيام جهة ذات ثقة عالية (هيئة الاعتماد) (Certificate Authority) على إنشاء وحدة استخراج هويات إلكترونية Certificate لكل من العميل والتاجر على أن تستخرج هذه الهويات بطريقة مضمونة بعد التأكد من هوية العميل ويتم حفظها وتداولها بطريقة مؤمنة وسرية، ويتمتع بالكثير من الضمانات منها:

- السرية من خلال تشفير مضمون الرسالة والمعلومات المالية بها.
- التحقق من شخصية كل من البائع والمشتري.
- حماية خصوصية العميل بعدم تتبع نوعية مشترياته.
- التكاملية وتعني ضمان أن الرسالة المرسلة هي نفسها الرسالة المستقبلة[2].

ثانيا- نظم أمن الحسابات المركزية:

بالنسبة لعالم الحسابات المركزية الكبيرة لا يوجد الكثير من نظم الأمن في الأسواق وربما السبب هو سيطرة بعض الشركات الكبرى على سوق الحسابات المركزية وتتميز هذه السوق بضخامة الإنتاج حيث يجب أن يكون نظام الأمن شاملة ومتناغمة مع نظام التشغيل الرئيسي ومع العديد من نظم التشغيل المساعدة ولذاك تحجم شركات نظم أمن المعلومات الصغيرة عن الدخول إلى هذه الأسـواق وتنـفرد به شركات مثل (IBM) لذلك

---

[1]- **إبراهيم بختي**، التجارة الإلكترونية، مفاهيم واستراتيجيات التطبيق في المؤسسة، المرجع السابق، ص79.

[2]- **نادر شعبان إبراهيم السواح**، النقود البلاستيكية وأثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، المرجع السابق، ص 124.

نجد على رأس نظم أمن الحسابات المركزية الشهيرة نظامان هما نظام "راكف" (RACF : Ressource Access Control Facility) ونظام Access Control Facility II[1].

ثالثا- نظم أمن الحسابات الشخصية: ومن بينها نجد:

1. **برنامج "بي سي سيف" (PC Safe)**:

الذي أنتجته شركة "إنيجما لوجيك" فهو برنامج يستخدم كلمة مرور لمرة واحدة فقط لتنظيم استخدام الحاسب فيقدم بذلك أسلوبا للتحكم في استخدام البيانات يطلق عليه (التحكم المحمول Portable Control)، إذ يمكن استخدام البيانات حيث يحدثون كلمة المرور التي تستخدم مرة واحدة، ولا يشترط أن يكون ذلك من خلال نظام التشغيل الذي تم من خلاله تشفير البيانات بل من خلال أي نظام تشغيل آخر. وهذا البرنامج يتطلب وسائل خاصة، يتيح استخدام كلمة المرور التي تستعمل لمرة واحدة وهذا العتاد محمول هو الآخر.

يسمح برنامج "بي سي سيف" بتشفير البيانات بواسطة المستخدم والاحتفاظ به في الصورة المشفرة ولا يمنع ذلك من استخدام من قبل مستخدمين آخرين، بافتراض أنهم مصرح لهم بذلك، فعند طلبها من المستخدم الجديد يتم فك تشفير أجزاء البيانات التي يحتاج إليها. فيقاوم هذا البرنامج محاولة اكتشاف كلمة المرور عن طريق التجربة والخطأ لأنه يتوقع كلمة مرور مختلفة في كل مر، وبذلك فإذا تمكن أحد المستخدمين من اكتشاف كلمة المرور الخاصة بمستخدم آخر لن تنفعه إذا أراد الدخول بها بعد خروج المستخدم الحقيقي لأن في هذه الحالة سيتوقع كلمة مرور جديدة.

2. **برنامج "إيزاك 2200" (Isac 2200)**:

هو من إنتاج إيزولشن سيستمز (Isolation systems) الكندية، فهو امتداد لنظام التشغيل (DOS)، فهو يفرض استخدام لمواصفات قياسية خاصة فيحتفظ بسجل كل ملف، أما بالنسبة للبرامج فيقوم البرنامج بتصنيف المستخدمين الذين يحق لهم استخدام كل

[1]- وهي عبارة أنظمة تتميز بمحدودية الاستعمال فهي أنظمة قليلة الانتشار لضرورة توافقها مع أنظمة منتجيها كشركة IBM. أنظر: **محمد دباس الحميد**، حماية أنظمة المعلومات، المرجع السابق، ص ص105-106.

برنامج ويفتح حق الاستخدام فقط للمستخدمين الذين تنطبق عليهم شروط الصلاحية المحددة بهذا السجل.

3. برنامج ديسك ووتشر (Watcher Disk):

فهو واحد من المجموعة التي صممت لحماية البيانات ولضمان عدم محوها عن طريق خطأ غير مقصود من جانب المستخدم[1].

4. برنامج ميل سيف (Mail Safe):

فهو برنامج مـن وضع شركة (RSA Security Data)، فيعتمد هذا البرنامج على تشفير الملفات من أجل تأمين الاتصالات وحالات التشارك في البيانات، وهو أكبر البرامج انتشارا ونفعا وجاذبية في حالات البريد الإلكتروني فهو يتيح ما نطاق عليه أغلفة رقمية وتوقيعات رقمية، أما الأغلفة الرقمية فهي تخفي معلومات عن الجميع ما عدى الجهة المقصود وصول الرسالة إليها، أما التوقيعات الرقمية فهي تنسب الرسالة إلى مرسلها الحقيقي وتمنع من أي تغيرات غير مرخص بها على الرسالة[2].

رابعا- تقنية الحماية 3DS:

وبهدف تطوير الدفع الالكتروني قامت مؤسسة فيزا بتطوير هذا النظام لتعزيز عملية الدفع عن طريق البطاقات الائتمانية، فهو نظام يوفر أعلى مستويات الحماية لعمليات الدفع عبر الإنترنت.

فيساهم في تخفيض نسبة الأخطار أو المشاكل التي تحدث خلال عملية الشراء عبر الإنترنت من خلال تمكين المصاريف المتخصصة في إصدار البطاقات والتحقق من هوية الشخص الذي قام بإجراء المعاملة التجارية الإلكترونية وتوفر تقنية "3 دي، أس" حماية إضافية حيث تتم العمليات الإلكترونية أمام الشخص مباشرة.

كما يعتمد على نظام التشفير (SSL) ومأخذ Merchant server لتمرير المعلومات والتأكد من هوية حامل البطاقة خلال عمليات الشراء التي تتم على الخط. ويجمع هذا

---

[1]- **محمد دباس الحميد**، حماية أنظمة المعلومات، المرجع السابق، ص ص106-107.

[2]- برنامج Watcher Disk يقوم على سبيل المثال باستبدال الأمر (Format) ويضع مكانه أمر آخر يتطلب تأكيد من المستخدم عند استخدامه، أنظر: المرجع نفسه، ص108.

النظام بين السهولة ومرونة التطبيق، ويوفر الانتقال الآمن لتفاصيل الحساب وتخفيض نسبة الأخطاء[1].

خامسا- تقنية الحوائط النارية (pare-feu):

وهي من أهم الأدوات الأمنية المستخدمة في تأمين الشبكات، ومنع الاتصالات الخارجية المرتبة في الإنترنت من الوصول إلى داخل الشبكة، فضلا عن قيامها بفترة الاتصالات الخارجية لبعض الخدمات المتوفرة على الشبكة الدولية[2].

فتعتبر حائط الصد الأمامي لجهاز الكمبيوتر الخاص بالمتعامل والذي يمنع التلصص على المعلومات الشخصية وما يحتفظ به على الحاسوب الشخصي، فهو نظام يسمح بحماية الحاسوب أو القناة التي يستعملها الحاسوب من التلصص عبر قنوات أو برامج أخرى خاصة الأنترنت المفتوحة على العالم.

يقوم هذا نظام بتصفية المعطيات المتنقلة عبر الشبكة فهو عبارة عن وسيط بين الحاسب الشخصي وشبكة الإنترنت فهو يقوم بمعالجة أو تحليل كل المعطيات والمعلومات المتبادلة بين المتعاملين المحليين والدوليين عبر هذه الشبكة[3].

فهي عبارة عن برمجيات تقوم بعدم السماح للأشخاص غير المسموح بهم للتعرض أو معرفة المعلومات الخاصة كأرقام بطاقات الدفع أو أرقام الحسابات أو كافة البيانات الأخرى التي تتميز بالسرية والشخصية والتي ما إذا تم تعديلها بشكل أو بأخر يتم إلحاق ضرر لمستعملها الشرعي.

---

[1] - **Steven J. Murdoch et Ross Anderson**, vérifié par visa et master Card Secure code, étude du laboratoire informatique, université de Cambridge, royaume uni, in: http://www.cl.cam.uk/users/. P2. Voir aussi : Tout système de paiement électronique sur internet passe par l'emploi du protocole SSL (secure socket layer) qui chiffre les données…pour que SSL fonctionne, un certificat (document électronique qui certifie qui vous êtes) est émis par une autorité de certification, c'est une organisation dont le rôle consiste à prouvé l'identité des entreprises voir: **Brenda Kieman**, E-commerce, stratégie α solutions, Microsoft presse, Paris, 2001, p250. Il est important pour le commerçant d'y joindre un système de vérification d'adresse. Malgré tout, les petite et moyenne entreprises ont l'avantage à utiliser SSL qui leur offre un mécanisme de paiement efficace voir aussi : **Pierre-Paul Lemyre,** le guide juridique du commerçant électronique, in : www.juristint.org

[2] - **أمير حيدر**، حماية الدفع الإلكتروني؟ مقال منشور على الموقع الالكتروني: www.islamonline.net2004/11/2، ص1.

[3]- Firewall (pare-feu) in:, www.commentaçamarche.net, 19/04/2009, 12.32, p.2.

وتعتبر تقنية الحوائط النارية كمراقب أو وسيط مراقب بين القناة الخارجية والبرمجيات الداخلية المتصلة فيما بينها حماية للمعطيات وانتقالها عبر قنوات الاتصالات خاصة الإنترنت. كما توجد العديد من البرمجيات والتقنيات الأخرى التي وضعت قصد حماية الدفع الإلكتروني التي تعتبر ركيزة ترقية وتطوير مجال التجارة الإلكترونية التي أصبحت حتمية في ظل العولمة المعلوماتية وضرورة التفتح للمعاملات الخارجية قصد تحقيق تعاون فعال وفعلي ما بين الدول.

المطلب الثاني

الحماية القانونية للدفع الإلكتروني

مع تزايد العمليات التجارية الالكترونية على المستوى العالمي والمستوى المحلي والتطور الكبير في الوسائل التقنية المستعملة لحماية التجارة الالكترونية كان من الإلزامي توفير الحماية التشريعية والقانونية لهذا النوع من التجارة، كان ولابد من إطار قانوني لبعث ثقة المستعملين بهذه التقنيات على المستوى الداخلي وذلك بتبني تشريعات تحمي المعاملات الإلكترونية بتبني الدول تشريعاتها الداخلية وقوانين تحمي مستعملي قنوات الاتصالات من وأشخاص معنويين مثل المؤسسات المالية أو البنوك والتجار التي توفر خدمة الدفع الالكتروني وأشخاص طبيعيين المستعملين لهذه التقنيات والوسائل أي المستهلكين.

وسنتعرض في هذا المبحث إلى الحماية الداخلية للدفع الإلكتروني وذلك بعرض مجموعة من النماذج للقوانين التي تبنتها الدول في تشريعاتها الداخلية سواء كانت حماية مدنية أو جنائية(فرع أول).

كما امتدت هذه الاهتمامات إلى ضرورة تضافر الجهود الدولية بوضع نصوص الحماية الإقليمية للمعاملات المالية خاصة في إطار الاتحاد الأوربي كما تمتد هذه الاهتمامات إلى النصوص الدولية المتعلقة بمجال الملكية الفكرية وذلك بتكييف وسائل التعامل الإلكترونية والبرامج التي تتم من خلالها هذه العمليات لأنها متصلة بالملكية الفكرية، فكان من الضروري إلى الإشارة أو دراسة الجهود الدولية القانونية في مجال

حماية المعاملات المالية الإلكترونية والمتمثلة أساسا في الدفع الالكتروني لضرورة التعاون لمواجهة مختلف المخاطر والجرائم التي تقلل من قيمة هذه المعاملات بالمواجهة الاتفاقية التي تعزز التصدي التقني أو الحماية التقنية التي سبقت دراستها في المبحث السابق نظرا لأهمية هذا الموضوع وحداثته خاصة على الدول التي استفادت من ثمار الثورة المعلوماتية(فرع ثان).

الفرع الأول

حماية التشريعات الداخلية للدفع الالكتروني

لقد تبنت الكثير من دول العالم تشريعات خاصة بحماية الدفع الإلكتروني في تشريعاتها الداخلية وذلك بسن قوانين تعاقب على الجرائم المعلوماتية حماية للمتعاملين عبر شبكات الاتصالات والقنوات المفتوحة ولقد مست ضرورة هذه التطورات الدول المتقدمة وكذلك الدول السائرة في طريق النمو، وسنقوم بدراسة الحماية القانونية في بعض الدول الأوربية. كما سعت الدول العربية منها الجزائر في طريق النمو نفس الحذو بتبنيها نصوص تشريعية وقوانين خاصة بالحماية القانونية من المخاطر والجرائم التي تمسها.

تعتبر الحماية التشريعية في الدول الأوربية مرجعا تشريعيا مهما في شتى المجالات وهذا يعكس التطور التكنولوجي والاجتماعي الذي تحظى به لذلك من الأجدر دراسة بعض النماذج التشريعية الأوربية الحامية لتداول البيانات.

أولا- في ظل القانون الفرنسي:

مرت التجربة الفرنسية في مجال الحماية التشريعية للمعاملات عبر شبكات الاتصالات عن بعد بعدة مراحل:

1- المرحلة الأولى:

كانت أولى المحاولات لمد سلطان قانون العقوبات لحماية المال المعلوماتي بفرنسا من طرف وزيرها للعدل وذلك سنة 1985، عندما تقدم بمشروع قانون عقوبات جديد. أضاف بموجبـه بابـا رابعا للكتاب الثالث منه بعنوان الجرائم على المادة المعلوماتية

(Les infractions en matière informatique) يتكون من ثمانية مواد من 1/307 إلى 8/307 تناولت بالتجريم الموضوعات التالية:

- التقاط البرامج أو المعطيات أو أي عنصر أخر من النظام المعلوماتي عمدا.
- استخدام أو نقل أو إنتاج برنامج أو معطيات أو أي عنصر من عناصر النظام بدون موافقة من لهم الحق.
- تخريب أو تعييب كل أو جزء من نظام المعالجة الآلية للمعلومات أو عرقلة أدائه لوظيفته .
- الحصول أو السماح بالحصول على فائدة غير مشروعة عن طريق الاستخدام غير المشروع لنظام المعالجة الآلية للمعلومات. لكن هذا المشروع لم يجد سبيله للتطبيق[1].

2- المرحلة الثانية:

هي المرحلة التي كللت بالنجاح فكانت في الخامس من أوت 1986 عندما تقدم النائب "Jacques Godfrain" ونواب آخرون إلى الجمعية الوطنية باقتراح مشروع قانون الغش المعلوماتي "Fraude informatique". هذا الاقتراح حاول تطوير وتعديل بعض النصوص في قانون العقوبات والتي تناولت الجرائم التقليدية كالسرقة وخيانة الأمانة والتزوير...، كما شملت العدوان على المال المعلوماتي، وتعددت مناقشات هذا المشروع في البرلمان الفرنسي. وأسفرت في النهاية عن قانون اختلف تماما عن ذلك المشروع والذي قدم أول مرة بل تشابه إلى حد كبير مع المشروع الأول الذي تقدم به وزير العدل عام 1985.

[1]- **محمد خليفة،** الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص66.

فتم إقرار هذا القانون وإدماجه في قانون العقوبات الفرنسي، ليشكل الباب الثالث من الكتاب من القسم الثاني منه وهذا الكتاب يتعلق بالجنايات والجنح الماسة للأشخاص. وأصبح الباب الثالث متعلقا بالجرائم المعلوماتية وذلك في المواد من 4/462 إلى 9/462 وتضمنت النص على الجرائم التالية[1]:

- الدخول أو البقاء غير المشروع في نظام معالجة آلية للمعطيات أو في جزء منه وتشديد العقوبة في حالة محو أو تعديل المعطيات الموجودة داخل هذا النظام أو إفساد وظيفته.
- إدخال معطيات في النظام أو محو أو تعديل المعطيات الموجودة فيه عمدا أو بدون مراعاة حقوق الغير، سواء تم ذلك بطريقة مباشرة أو غير مباشرة.
- كل فعل من شأنه أن يعرقل أو يفسد عمدا أو بدون مراعاة حقوق الغير أداء النظام لوظيفته.
- تزوير المستندات المعالجة آليا أي كان شكل واستعمال هذه المستندات.
- الشروع في ارتكاب الجرائم السابقة.
- الاتفاق الجنائي على ارتكاب الجرائم السابقة.

كما جرم المشرع الفرنسي في المادة 11 من القانون 91-1382 الصادر في 30 ديسمبر 1991 بعض صور الاستعمال غير المشروع للبطاقة وهي تقليد أو تزوير بطاقة من بطاقات السحب واستعمال أو محاولة استعمال البطاقة المقلدة أو المزورة وقبول الوفاء عن طريق بطاقة دفع مقلدة أو مزورة مع العلم بذلك.

3-المرحلة الثالثة:

فكانت في سنة 1994، عندما تم تعديل قانون العقوبات الفرنسي، وقد استخدم هذا التعديل مصطلح الغش في الجرائم السابقة واستغنى عن مصطلح "دون مراعاة حقوق

1- فوصلت عدد المناقشات إلى ثلاثة أمام الجمعية الوطنية ومرتين أمام مجلس الشيوخ، وطال أمدها استغرقت عاما ونصف عام. أنظر: **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص67.

الغير"، كما أن هذا التعديل مس المادة 1/441، فطور من جريمة التزوير المعلوماتي لتصبح جريمة تزوير المستندات المعالجة آليا فحسب.

وبذلك تم إخراج هذه الجريمة من نطاق جرائم الاعتداء على نظام المعالجة الآلية للمعطيات لاختلاف المصلحة المحمية فيها عن المصلحة في تلك الجرائم. فهي في هذه الأخيرة مصلحة صاحب الحق في النظام ومن له حق السيطرة عليه بينما في جريمة التزوير المعلوماتي الجديدة هي الثقة[1] العامة في المستندات ذات القيمة القانونية أي كان شكلها وقد ضم هذا التعديل المواد من 1/323 إلى 7/323[2]. وفي نص المادة 3/323 لا يحمي المشرع الفرنسي بهذا النص النظام من الناحية المادية، ولكنه يوفر بهذا النص الحماية للبيانات الموجودة في النظام من أي نشاط إجرامي وتتضمن هذه الجريمة صور ثلاثة: الإدخال، المحو والتعديل.

ولا يشترط أن تتوافر هذه الصور جميعها، بل يكفي لتحقق الجريمة أن تتوافر إحداها، وموضوع الجريمة هو المعلومات التي تم معالجتها إلكترونيا، وهو ما يعني شمولها لكافة البيانات الواردة في المستندات الإلكترونية[3]. وبعد 10 سنوات من هذا التعديل جاء تعديل آخر لقانون العقوبات الفرنسي سنة 2004. وقد أضاف المشرع بموجبه جريمة أخرى وهي جريمة التعامل في وسائل يمكن أن ترتكب بها جريمة، أي تلك الوسائل التي تصلح لأن ترتكب بها جريمة الدخول أو البقاء غير المصرح بهما أو جريمة التلاعب بالمعطيات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات وقد نصت على هذه الجريمة المادة 3/232-1[4].

---

[1]- **محمد خليفة،** الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص ص68-69.

[2]- Voir le code pénal français, crée par la loi no 96-392 du 13 mai 1996- JORF mai 1996 in : http://droit-finance-commentcamarche.net/legifrance/37-codepenal.

[3]- **محمد خليفة،** الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص69.

[4]- كما أن تعديل قانون العقوبات سنة 1994 أقر مسؤولية الشخص المعنوي بعدما كان الفقه والقضاء الفرنسيين منقسمين بشأنها بسبب سكوت قانون العقوبات الفرنسي لسنة 1810 عن هذا القانون بعدما كان قانون 1670 يقر هذه المسؤولية، وظل هذا الجدل قائما حتى صدور قانتون العقوبات لسنة 1994 الذي أقر مسؤولية الشخص المعنوي.

أنظر في ذلك: نصوص المواد 1/323 إلى 7/323 من القانون 275/2004، المؤرخ في 25 جوان 2004، الجريدة الرسمية 22 جوان 2004 المعدل لقانون العقوبات الفرنسي.

وتنص المادة 1/323 من القانون 275/2004 على أنه بمجرد الدخول أو البقاء بصفة غير قانونية في كل أو جزء من نظام المعالجة الإلكترونية للبيانات معاقب بسنتين حبس وبـ 30.000 أورو غرامة عندما ينتج من جراء ذلك سواء محو أو تغيير البيانات التي يحتويها النظام، كما يشدد العقوبة في حالة عرقلة سير النظام.

كما نصت المادة 3/323 من نفس القانون والمعدل لقانون العقوبات الفرنـسي على أنّه بمجرد إضافة أو إدخال بطريقة غير شرعية بيانات في نظام المعالجة الرقمية أو محو أو تغيير غير شرعي للبيانات التي يحتويها معاقب على هذه الأفعال بـ خمس سنوات حبس و750.000 أورو غرامة.

كما نصت المادة 5/323 على العقوبات الإضافية إلى جانب العقوبات الأصلية فالأشخاص الطبيعة التي تقترف هذا النوع من الجرائم أي الجرائم المعلوماتية، تحرم من حقوقها المدنية والعائلية لمدة 5 سنوات. ويتم حجز كل الوسائل التي ساعدته على اقتراف هذه الجريمة، كما يتم إقصاؤه من الصفقات العمومية لنفس المدة. كما اعتبرت المادة 7/323 أن محاولة اقتراف المخالفات أو الجرائم التي نصت عليها المواد 1/323 و3/323-1 معاقب عليه بنفس العقوبات[1].

4-المرحلة الرابعة:

الحماية في قانون السيرة الجيدة (Code de la bonne conduite) كما نجد في فرنسا الكثير من القوانين التي سنت من أجل حماية المستهلك الذي يتعامل من خلال التجارة الإلكترونية والعقود عن بعد. وإلى جانب النص على الحماية القانونية في قانون العقوبات سنت قوانين من أجل تدعيم هذه الحماية لضمانها طريقة تعليل أفضل وأنجع.

فنجد من بين هذه القوانين القانون 1062-2001 المؤرخ في 15 نوفمبر 2001 والمتعلق بالحماية الدائمة والتي أدخلت في القانون النقدي والمالي نصوصا جديدة قصد

[1]- **محمد خليفة،** الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص69.

ضمان حماية الدفع الذي يتم ببطاقة الدفع. والتي تمنح لبنك فرنسا مهمة ضمان حماية وسائل الدفع[1].

لذلك يستلزم أن تحظى بطاقات الدفع بحماية قانونية جنائية على غرار ما فعل المشرع بالنسبة للشيك ويمكن تحديد الأفعال موضوع التجريم في الآتي:

- تقليد وتزوير بطاقة الدفع واستعمالها.
- صناعة أو بيع أو عرض للبيع أو حيازة أدوات أو آلات مما يستعمل في تصنيع البطاقات بغير ترخيص قانوني.
- صناعة أو بيع أو عرض للبيع أو حيازة الأدوات أو الآلات الخاصة بنظام الدفع بغير تصريح قانوني.
- استخدام بطاقة صحيحة أو ملغاة أو منتهية في سحب مبلغ تتجاوز الرصيد أو في الوفاء لدى التجار مع عدم وجود رصيد[2].

ثانيا- في القانون الألماني:

توجد القليل من القواعد التشريعية والتنظيمية الخاص بضمان حماية المعاملات الإلكترونية (بواسطة بطاقة الدفع) فتعتبر معظم هذه النصوص في التشريع الألماني عبارة عن قواعد عامة والتي تستلهم من قانون العقود بحيث يعتبرها البعض مرنة بالقدر الكافي لتغطية الحالات الخاصة من بينها العلاقة بين حامل البطاقة من جهة والتجار أو المؤسسات المالية من جهة أخرى.

وبدخول قانون الشراء عن بعد حيز التنفيذ في أول جويلية 2000 الذي جاء مساير للتعليمة الأوربية 97/7، أدخلت العديد من إجراءات الحماية الخاصة لاستعمال بطاقات الدفع وقد تم بعد ذلك إلغاء قانون الشراء عن بعد في 31 ديسمبر 2001 حينما أدخلت قواعدها في القانون المدني الألماني.

---

[1]- Document du service des études juridiques du senat(RF),La sécurité des transactions réalisées par carte bancaire, in : http://www.senat.fr/lc/lc125.html, Octobre 2003, p.01.

[2]- **بسمة رزق**، المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقة الدفع، بحث منشور على الموقع: http://www.mn940.net/forum، 28-06-2009، ص1.

وقد نص قانون العقوبات الألماني على جملة من الأفعال المجرمة في هذا المقام. فتنص المادة 152A من نفس القانون أنه بمجرد استعمال بطاقة مزورة أو حيازتها أو إعطاؤها لشخص آخر والتي تدخل في نطاق هذه المادة يعاقب بمدة حبس تتراوح ما بين سنة إلى 10 سنوات. وعندما تكون هذه الجريمة مرتكبة من طرف مجموعة تكون العقوبة الأدنى بسنتين.

كما نص على الاستعمال المفرط لبطاقات الدفع بموجب نص المادة 266B من قانون العقوبات أنها تكيف جريمة ذات خصوصية معاقب عليها بغرامة أو بعقوبة الحبس لمدة لا تتجاوز ثلاثة سنوات، وتعتبر الجريمة بموجب نص المادة 266B الاستعمال للبطاقة من قبل حاملها الشرعي والذي أحدث ضررا لمصدر البطاقة والتي يكون الغرض منها سحب أموال سائلة عن طريق الموزعين الآليين التابعين لمجموعة من المؤسسات العالمية.

كما تم النص على الاستعمالات التعسفية الأخرى من قبل صاحبها في المادة 263A من قانون العقوبات والخاصة بالتزوير الرقمي (الجريمة المعلوماتية) بحيث يعاقب عليها بغرامة وخمسة سنوات حبس على الأكثر.

كما اتخذت البنوك منذ أفريل 2001 إجراء يستلزم على المستهلكين تقديم للبائعين عددا يتكون من ثلاثة أرقام والمتواجدة على ظهر البطاقة عند دفعه للسلع أو الخدمات التي اقتناها.

كما سعى البائعون ومقدمو الخدمات إلى فرض مراقبات عديدة، فيفرض على المشتري تقديم بطاقة الهوية عند استعمال بطاقة الدفع ويفرض على الآخرين تقديم الرقم السري حتى ولو تم توقيعه على الفاتورة. كما يوجد تعاون داخلي ما بين أجهزة الشرطة والمتعاملين بهذه الطريقة وذلك بتقديم الأرقام المسروقة من قبل من المعاملات المزورة[1].

1- Document du service des etudes juridiques du senat(RF),La sécurité des transactions réalisées par carte bancaire, in : http://www.senat.fr/lc/lc125.html, Octobre 2003, p.02.

ولم يتوقف المشرع الألماني عند هذا الحد، فنص في المادة 270 من قانون العقوبات على أن يعاقب كل من توصل بطريق الخداع إلى إحداث تأثير يؤدي إلى الإخلال بعمل نظام البيانات الإلكترونية.

فيهدف من خلال ذلك إلى حماية نظم معالجة البيانات وقيامها بدورها، ويقصد بالمساس إدخال بيانات إضافية أو محوها لا يعني أن تكون بصدد صورة من صور تزوير هذه البيانات وإنما الأثر الذي يحدثه هذا المساس بتلك البيانات كإتلافه وعدم قدرته على القيام بعمله الذي وضع من أجله[1].

ثالثا- في القانون الجزائري:

لقد تسارعت وتيرة الاعتماد على المعلوماتية في شتى المجالات حتى باتت ضرورة لا يمكن الاستغناء عنها، وأصبحت مقياسا لتطور الدول، والجزائر ليست بمنآى عن هذا التحول المعلوماتي، الذي حمل في طياته مصالح جيدة غير تلك التي يحميها قانون العقوبات، فبدت الحاجة شديدة لوضع نصوص جديدة.

ولقد جاء في عرض أسباب هذا التعديل لقانون العقوبات أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها، والجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وذلك لسد الفراغ القانوني في بعض المجالات.

وكان التعديل بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبـر 2004 المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات والذي أفرد القسم السابع مكرر منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" والذي تضمن ثمانية مواد من المادة 394 مكرر حتى المادة 394 مكرر7[2].

---

[1]-**Francis Lorentz**,commerce électronique, une nouvelle donnée pour les consommateurs, les entreprises, les citoyens et les pouvoirs public, in : http://www.minefi.gouv.fr/fonddocumentaire/ p7.

[2]- **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص62.

نصت المادة 394 مكرر المضافة بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 على: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 د.ج إلى200.000 د.ج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة من ستة أشهر إلى سنتين والغرامة من 50.000 د.ج إلى 300.000 د.ج".

وتضيف المادة 394 مكرر1 من القانون نفسه على أنه: "يعاقب بالحبس من ستة (6)أشهر إلى ثلاثة سنوات وبغرامة من 500.000 د.ج إلى 4.000.000 د.ج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[1].

كما نص هذا التعديل أيضا على عقوبة مصادرة وسائل ارتكاب الجريمة وإغلاق المواقع التي تكون محلا لها، وإغلاق المحل أو المكان الذي ارتكبت فيه الجريمة وفقا لنص المادة 394 مكرر6، كما عاقب التعديل على الشروع في جرائم هذا القسم.

وكانت مواجهة الجريمة المعلوماتية إحدى بنود اتفاق يؤسس شراكة بين الاتحاد الأوروبي والجزائر، عقد بتاريخ 22 أفريل 2002، وتضمنت ذلك المادة 86 منه[2].

وتماشيا مع متطلبات البنك الإلكتروني من تنظيم وتسخير وسائل خاص بالتعامل بها احتضن مركز البحث وتسيير الإعلام التقني التابع لبنك الفلاحة والتنمية الريفية يوما مهنيا حول موضوع البنك الإلكتروني، حضره مجموعة من رجال الإعلام الآلي ومختصون في الاتصال البنكي.

نظم هذا اليوم تحت إشراف MAGACT بمشاركة المؤسسات الفرنسية المختصة في هذا المجال ولقد استهل اللقاء بطرح إشكالية إيجاد سياسة تسمح بتطبيق البنك الإلكتروني

---

[1]- المواد 394 مكرر و394 مكرر1 من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات.

[2]- **محمد خليفة،** الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص63.

ثم في مرحلة ثانية، اقتراح القواعد والأسس التي يقوم عليها النظام فعرض تطبيقي يبرز فعالية هذه التكنولوجية الجديدة.

تساؤلان أساسيان شكلا محور اهتمام الحاضرين يدوران حول حماية وفعالية هذا النظام الجديد، فخطر القرصنة حسب أحد المتدخلين ضعيف لكنه لا يعزل هذا بالإضافة إلى مشكلة الفراغ القانوني الذي يعاني منه توظيف هذا النوع من التكنولوجيا[1].

وسارت في هذا المسار السياسة البنكية الجزائرية من أجل ضمان عمليات الوفاء الإلكتروني، وفي هذا الشأن أصدر بنك الجزائر تنظيم داخلي رقم 05-07 بتاريخ 28 ديسمبر 2005، يتعلق بأمن أنظمة الوفاء. فهذا التنظيم يعرف النظام بين بنكي للدفع أو التسوية، وهو عبارة عن إجراءات وطنية أو دولية، تنظم العلاقات بين طرفين على الأقل تتوفر فيهم صفة بنك أو مؤسسة مالية أو مؤسسة منخرطة في غرفة المقاصة.

يتعين على كل عضو في هذا النظام أنه يجب عليه أن يتخذ الإجراءات، كل فيما يخصه، والمتعلق بمعايير نظام المواكبة للقواعد الدولية في هذا المجال.

تقوم فكرة أمن أنظمة الدفع أساسا على ضمان البنية التحتية للنظام ووسائل الدفع المختلفة. ويتعلق الأمر بالبنية التحتية، المكونات المركزية للإنتاج،التجهيزات التقنية تجهيزات سواء التجهيزات أو البرامج الموضوعة تحت تصرف المشتركين المعتمدين ومدى النجاعة العملية للبنية التحتية، خاصة ما يتعلق بالاتصالات والطاقة الكهربائية (المادة4) أمن المنشآت والأنظمة تتضمنها المادة (5) كما يلي :

- جاهزية الأنظمة (La disponibilité des systèmes) .
- تثبيت المعلومات المتبادلة (L’intégrité des données échangées).
- ترك أثار المعلومات المتبادلة (La traçabilité des données échangées) .
- السرية (La confidentialité) .
- إمكانية المراقبة (L’auditabilité) [2].

1- BADR Info, Revue bimestrielle d’information, N° 33, Mars-Avril, 2003.

2- **عبد المجيد قادري** ، الوفاء الإلكتروني مجلة العلوم القانونية، جامعة باجي مختار عنابة، العدد 12، جوان 2008 ص ص168-169 .

ولضمان حماية فعالة للعمليات الالكترونية، بادرت هيئة التنظيم التابعة للبريد والمواصلات في الجزائر إلى إعداد مشروع حول الشهادة الالكترونية لتامين المعاملات عبر شبكة المواصلات.

ترجم هذا المشروع بتنظيم مناقصة وطنية ودولية مفتوحة في 06 سبتمبر2009 تهدف من خلالها إيجاد شركة مختصة في ميدان الشهادات الالكترونية، والتي تكلف أساسا بوضع الأدوات والميكانيزمات اللازمة لإنشاء ومتابعة استعمال الشهادات الالكترونية أثناء تبادل البيانات عبر الانترنت.

وقد تم سحب دفتر الشروط من طرف 21 شركة مختصة، ورغم إتمام فتح العروض المقدمة من طرف ثمانية شركات، إلا انه لم يتم إلى حد الآن المنح النهائي للصفقة، وهذا راجع لحساسية المشروع ورغبة السلطات المحلية في فرض رقابة فعالة على المشروع، إلاّ أن حسب تصريحات أحد مسؤولي المشروع من الممكن أن تخول الصفقة للشركة الفرنسية(Keynetics) [1].

كما تضمن القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي نص في المادة الأولى منه أن الهدف الذي وضع من أجله هو وضع قواعد خاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

حصر القانون نفسه في المادة الثانية فقرة **أ** هذه الجرائم، بتلك الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات.

وأنشأ القانون09-04 في الفصل الخامس منه هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وخولت لها المادة 14 المهام الآتية:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

---

[1] **-T.H**, le projet de certification électronique n'a toujours pas abouti, malaise à l'ARPT. Article, le soir d'Algérie, quotidien indépendant, dimanche 06/06/2010, p4.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم[1].

ويمكننا الإشارة في هذا الشأن كذلك إلى القوانين الخاصة بحماية الملكية الفكرية ففي الجزائر على سبيل المثال نجد الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة وفي الفصل الخاص بالخدمات المحمية وفي المادة الرابعة فقرة أولى أشارت إلى برامج الحواسيب ضمن نطاق الملكية الفكرية المحمية والتي يعاقب على التعدي عليها من طرف الغير دون رخصة من مالكها الأصلي[2].

واعتمادا على ذلك يمكن استخلاص أن المشرع الجزائري قد وسع من مجال الحماية إلى أن يمس كافة الجرائم سواء الماسة بأمن الدولة، الجرائم الالكترونية الماسة بالاقتصاد الوطني أو المتعلقة بالأخلاق، من خلال عبارة "أي جريمة أخرى...".

كما يمكننا اعتبار الاعتداء على شبكات الاتصالات الخاصة بمواقع البنوك والعمليات النقدية الالكترونية بين المنشآت التجارية والاقتصادية من قبيل الجرائم الماسة بالاقتصاد الوطني. ويتماشى هذا القانون مع الطبيعة الدولية للجريمة الالكترونية، التي

---

[1]- المواد 1و2 و14 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، الجريد الرسمية ر قم 47-2009 المؤرخة في 25 شعبان عام 1430 الموافق 10 غشت 2009.

[2]- المادة 1/4 من الأمر 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية رقم 44 المؤرخة 2003/07/23.

ونشير إلى أن الجزائر وقعت بموجب الأمر 75-02 المؤرخ في 1975/01/09 على اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 20 مارس 1883، التي تمت مراجعتها عدة مرات أخرها في ستوكهولم 1967/07/14 والتي تنص في المادة2/1 منها: حماية الملكية الصناعية تخص براءة الاختراع، نموذج الاستعمال، الرسم والنماذج الصناعية، علامات الصنع والعلامات التجارية، علامات الخدمات...الخ .أنظر في ذلك:

Mabrouk Hocine, code de la propriété intellectuelle, édition Houma, 1er édition, Alger, 2007, p11.

ترتكب عادة في بلد معين إلاّ أن آثار الجريمة تكون في بلد مغاير، الشيء الذي يستدعي ضرورة التنسيق بين هيئات مكافحة مرتكبيها.

الفرع الثاني

التعاون الدولي لحماية الدفع الإلكتروني

لم تتوقف ضرورة حماية الدفع الإلكتروني قصد ترقية التجارة الإلكترونية على التشريعات الداخلية للدول فقط، وإنما تجاوز ذلك الاهتمام إلى تضافر الجهود الدولية قصد وضع إطار قانوني يضمن حماية هذا النوع من المعاملات وحماية المستهلك خاصة جراء الدفع الذي يقوم به عبر الخط وسنقوم بدراسة بعض النماذج الإقليمية والدولية لترسيخ وحماية الدفع الإلكتروني.

أولاً- في ظل الاتحاد الأوروبي:

يعود الاهتمام الأوربي بالحماية التشريعية للمعاملات الإلكترونية إلى المجموعة الاقتصادية الأوروبية (CEE) التي سعت وراء ضرورة حماية الدفع الإلكتروني ويظهر ذلك من خلال التوصية رقم 598/87 التي وضعتها اللجنة الأوروبية في 8 ديسمبر 1987 حول القانون الأوروبي للسيرة الحسنة الخاصة بالدفع الإلكتروني. هذه التوصية تدعو كافة المتعاملين للمثول لهذا القانون من أجل ترقية الحماية والضمان للمستهلكين، الحماية والمردودية المتواصلة ما بين مقدمي الخدمات ومصدري هذا النوع من وسائل الدفع فيما بينها قبل تاريخ 31 ديسمبر 1992 وكذلك ملائمة كافة نهائيات الدفع مع كافة البطاقات البنكية التي تتداول في السوق.

كما تنص على إضفاء الطابع الشخصي والسري للمعطيات أو البيانات المقدمة من طرف المستهلك، حق الدخول المتساوي إلى كافة خدمات مقدمي خدمات الدفع الإلكتروني.

كما حرص على التزام المستهلك أو حامل البطاقة على ضرورة الأخذ بالعناية اللازمة طريقة استعمال بطاقة الدفع[1].

---

[1]- Recommandation 87/598/CEE de la Commission Européenne du 8-12-1987 portant sur un Code Européen de bonne conduite en matière de paiement électronique, JOL 365, 24-12-1987.

وصدرت كذلك عن الاتحاد الأوروبي التوصية رقم 489/97 في 27 جويلية 1997 والمتعلقة بالمعاملات التي تتم بواسطة وسائل الدفع الإلكتروني وخاصة تنظيم العلاقة بين مصدر البطاقات والحامل. فتطبق هذه التوصية في مجملها في المعاملات التي تتم بوسائل الدفع الإلكتروني عن بعد منها:

- انتقال الأموال المتعلقة باستخدام وسائل الدفع الإلكتروني.

- سحب الأموال السائلة بواسطة وسيلة دفع إلكترونية، وسيلة النقود الرقمية والتي تتم في آلات السحب الآلي للأوراق أو غيرها.

كما حرصت هذه التوصية على ضرورة استعمال وسائل الدفع الإلكتروني بالطريقة الصحيحة وفقا للشروط المتفق عليها باستعمال أو إصدار هذه الوسائل وأخذ كافة الاحتياطات اللازمة لحماية هذه الوسائل(1).

ثانيا- اتفاقية المجلس الأوروبي الخاصة بالجريمة المعلوماتية:

والتي افتتح باب التوقيع عليها في 23 نوفمبر 2001، حيث تهدف هذه الاتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق وانسجام التشريعات الوطنية بعضها البعض وتعزيز من قدرات القضاء والتشدد في تطبيق القانون وتقوية وتحسين التعاون الدولي في هذا الإطار.

وكذلك العمل على تعريف وتحديد العقوبات من جرائم المعلوماتية في إطار قوانينهم المحلية(2)، وباستقراء هذه الاتفاقية نجد في ديباجتها الكثير من الجرائم المعلوماتية ومنها الخاصة بحماية البيانات الشخصية في مجال الخدمات المتعلقة بالاتصالات السلكية واللاسلكية.

---

[1]- Recommandation 97/489/CE du 30 juillet 1997 concernant les opérations effectuées au moyens d'Instruments de paiement électronique, relation entre émetteur et titulaire J.O L 208 du 02/08/1997, in : http://europa.eu/legislation-séminaire/international.

[2]- **عماد يوسف حب ا** ، حماية الفضاء السبيراتي – الأمور التنظيمية لأمن المعلومات والاتصالات-، الهيئة المنظمة للاتصالات في لبنان: أمن الفضاء السبيراتي، 4-5 شباط 2009، مقال منشور على الموقع: http://www.tra.gov.lb/library، ص10.

وقد تم تحديد الجرائم التي تمس سرية، وأمن وسلامة وتوافر بيانات الكمبيوتر ومنظوماته في المادة الثانية منها من الفصل الثاني الذي يحمل عنوان الإجراءات الواجب اتخاذها على الصعيد الوطني، وقد حصرت هذه المادة هذه الجرائم في:

- الدخول غير المشروع على منظومة الكمبيوتر كليا أو على جزء منها دون وجه حق.

- الاعتراض غير المشروع لحظة سير البيانات دون وجه حق وعن قصد باستخدام الوسائل الفنية لقطع عمليات البث والإرسال، ونصت على ذلك المادة 03 من الاتفاقية.

- ونصت المادة 04 على التدخل في البيانات، عند ارتكابها عن قصد، وذلك من حيث إتلاف، أو إلغاء، أو إفساد، أو تغيير، أو تدمير البيانات الموجودة بالكمبيوتر دون وجه حق.

وذكرت المادة 07 الجرائم المتعلقة بالكمبيوتر وذلك عند ارتكابه عن قصد وبدون وجه حق وذلك من حيث تزويد الكمبيوتر ببرامج خاصة للاعتداء على المعلومات والبيانات المتداولة عبر قنوات الاتصال، بتبديلها أو تغييرها أو إلغائها باستعمال الكمبيوتر، مما ينتج عنه وجود معلومات وبيانات غير صحيحة بقصد دراستها أو الاهتمام بها و استعمالها لأغراض غير قانونية كما لو كانت صحيحة[1].

وقصد حماية النشاط الإلكتروني وردع الجرائم التي تتم بالطرق الإلكترونية والتي تمس بنشاط معين أقرت الاتفاقية على ضرورة قيام الدول الأطراف فيها بإقرار الإجراءات التشريعية وغيرها من الإجراءات الأخرى كلما كان ذلك ضروريا للحفاظ على السير الحسن في إطار القانون للنشاطات الاقتصادية التي تتم باستعمالات الحواسيب.

ويمكننا الاستنتاج أنه لو لم تنص صراحة على الجرائم المعلوماتية الخاصة بالتجارة يمكن استنتاج ذلك ضمنيا وذلك بطبيعة التجارة الإلكترونية التي تجرد من الطبيعة المادية للمعاملات والتي تترجم عن طريق بيانات التي ترسل عبر قنوات الاتصال المختلفة.

---

[1]- راجع المواد 2-4 و7 من اتفاقية المجلس الأوروبي الخاصة بالإجرام السبيري، بودابست، 23-11-2001.

ولقد بينت اتفاقية المجلس الأوروبي في المادة 23 منها على الأسس العامة المتعلقة بالتعاون الدولي، بحيث ذكرت تعاون الدول الأطراف فيها مع بعضها البعض من خلال تطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية والإجراءات المتفق عليها بمقتضى التشريع الخاص بالتماثل أو المتعلق بمبدأ المعاملة بالمثل.

واستجابة القوانين الوطنية المحلية لأقصى درجة ممكنة للأغراض الخاصة بعمليات التحقيق والبحث أو الإجراءات المتعلقة بالجرائم أو الخاصة بنظم وبيانات الكمبيوتر، أو لتجميع الأدلة الخاصة بالجريمة في صورة إلكترونية[1].

ويمكننا القول أن هذه الأسس المقررة من أجل تحقيق تعاون دولي لوضع حد للجرائم المعلوماتية وحماية مستعملي الإنترنت استجابة لخصوصية التجارة الإلكترونية التي لا تخضع للمفهوم الكلاسيكي للحدود، وذلك راجع لتفتح قنوات الاتصالات على العديد من دول العالم في آن واحد، والتصدي لهذه الجرائم ولو اختلف مكان آثارها عن مكان اقترافها كسرقة بيانات أو تغييرها من بلد معيين وتضرر أشخاص موجودين في بلد آخر من جراء ذلك الفعل، وبالتالي ضرورة تضافر جهود كافة الدول لتحقيق تعاون فعلي وفعال في عصر تكنولوجيا الاتصالات وثورة المعلوماتية.

ولقد جاء في المذكرة التفسيرية لاتفاقية بودابست الموقعة في 23 نوفمبر 2001:
«... كما أن الاستخدام العام للبريد الإلكتروني ووصول الجمهور لمواقع الويب عبر الإنترنت من أمثلة هذا التطور الذي قلب أوضاع مجتمعنا. كذلك فإن سهولة الوصول إلى المعلومات في النظم المعلوماتية مع الإمكانيات اللامحدودة لتبادلها وإرسالها بصرف النظر عن المسافات الجغرافية... ومن خلال الاتصال بخدمات الاتصالات والمعلومات يستطيع المستخدمون اصطناع فضاء جديد يسمى الفضاء المعلوماتي الذي يستعمل أساسا لآثار شرعية ولكن يمكن أن يخضع لسوء الاستخدام. إذ هناك احتمال لاستخدام شبكات الحاسوب والمعلومات الإلكترونية في ارتكاب أعمال إجرامية.

---

[1]- راجع المادة 23 من اتفاقية المجلس الأوروبي الخاصة بالإجرام السبيري، بودابست، 23-11-2001.

وعلى ذلك يجب على القانون الجنائي أن يحافظ على مواكبته لهذه التطورات التكنولوجية التي تقدم فرصا واسعة لإساءة استخدام إمكانيات الفضاء المعلوماتي...»[1].

ثالثا- جهود الاتحاد الدولي للاتصالات لحماية الفضاء الإلكتروني:

وقد وضع مجموعة توصيات بين فيها مجموعة الأطر التنظيمية والإجراءات العملية والتقنيات والتكنولوجيات الهادفة إلى منع الاستعمال غير المصرح به، مع تحيد السبل المسموح بها لاستعمال المعلومات وأنظمة الاتصالات الإلكترونية مع التشديد على مبادئ:

- تأمين استمرارية الخدمة.
- خصوصية المعطيات والمعلومات.
- الحرص على إيجاد السبل الكفيلة بحماية المواطنين والمستخدمين لهذه التقنيات من كافة المخاطر التي قد تتأتى من استعمالها واختراق الشبكات بهدف سرقة المعلومات والأسرار الحساسة.

- الأضرار المتأتية من الجهل وسوء الاستعمال ومن بعض المستخدمين المرخص لهم الذين يستغلون مراكزهم للقيام بأعمال غير مرخص لهم بها.

فتهدف هذه التوصيات إلى حماية الاقتصاد بشكل عام وكذلك حماية البيانات والمعلومات المخزنة وأنظمة المعلومات كما تساهم على الحفاظ على ثقة المستخدمين وتحقق هذه الأهداف برفع مستوى التوعية حول المخاطر الموجودة، إنشاء مؤسسات وإطارات وطنية تعتني بموضوع إيجاد وسائل الحماية والتوعية من المخاطر.

كما دعت التوصية إلى مواجهة التحديات عبر تضافر جهود وعوامل، الأفراد والقوانين والأطر التنظيمية، والإجراءات العملية والتكنولوجيا، كما يجب على الأفراد أن يكونوا حريصين على إتباع الإجراءات المرسومة من قبل المؤسسات المعنية[2].

---

[1]- **محمد خليفة،** الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص 73.

[2]- **عماد يوسف حب ا** ، حماية الفضاء السبيراتي – الأمور التنظيمية لأمن المعلومات والاتصالات-، الهيئة المنظمة للاتصالات في لبنان: أمن الفضاء السبيراتي، 4-5 شباط 2009، مقال منشور على الموقع: http://www.tra.gov.lb/library.

- على المؤسسات وضع إجراءات حماية فعالة والتشدد في تطبيقها.
- على مؤسسات القطاعين العام والخاص أن تحرص على استخدام طبقات متعددة من تقنيات الحماية واعتماد تكنولوجيات متعددة للحد ما أمكن من المخاطر.
- تقييم وفهم المخاطر واستخدام وسائل خاصة للحماية.
- ومن بين إجراءات الحماية كذلك أوصت بـ :
- التركيب والصيانة بطرق سليمة.
- استخدام الجدران النارية مع كلمات السر.
- الترميز والتشفير، زيادة استخدام التشفير على شبكة الإنترنت، على سبيل المثال مع الشبكات الافتراضية الخاصة(VPNS) وبرامج حماية برتوكولات الإنترنت (IPSEC).
- إعطاء دور أمن أوسع لمديري الشبكات.
- الاستعانة بأصحاب الخبرة الأجنبيين.
- عمليات مراجعة وتدقيق دورية إجراءات الحماية والأمان.
- الحد ما أمكن من عدد الأشخاص الذين يحق لهم الوصول إلى غرف الحاسوب(1).

كما هدفت توصيات الاتحاد الدولي للاتصالات إلى سن مجموعة متكاملة من القوانين المتعلقة بالفضاء الإلكتروني وأمنه مع وضعها موضع التنفيذ، على أن تتوافق هذه القوانين مع أحكام الاتفاقات العالمية لمكافحة جرائم المعلوماتية ويترجم ذلك بإجراء تقييم لمدى كفاية القدرات الراهنة للسلطات القضائية يدعي لمراجعة قوانينه الجنائية الراهنة لتحديد مدى كفايتها لمعالجة المشاكل المالية والمستقبلية لجرائم المعلوماتية.

- اعتماد قوانين إجرائية وأسس تعاونية وسياسات موضوعية لمكافحة فاعلة لجرائم المعلوماتية.
- إنشاء وحدات وطنية مختصة بمكافحة جرائم المعلوماتية(2).

1- الموقع نفسه.

2- **عماد يوسف حب ا** ، حماية الفضاء السيبراتي – الأمور التنظيمية لأمن المعلومات والاتصالات-، الهيئة المنظمة للاتصالات في لبنان: أمن الفضاء السيبراتي، 4-5 شباط 2009، مقال منشور على الموقع: http://www.tra.gov.lb/library.

رابعا- الحماية في ظل المنظمة العالمية للتجارة:

إن اهتمام المنظمة العالمية للتجارة بموضوع التجارة الإلكترونية يمس بدون شك بالجزء الذي يعتبر موضع دراستنا وفي هذا السياق أشارت في الإعلان الوزاري الذي تمخض عن الندوة الوزارية للمنظمة العالمية للتجارة في دورة الدوحة 2001، أنها أخذت بعين الاعتبار كافة الأعمال التي قام بها المجلس العام والتي يدعمها الكثير من الهياكل والتي تعتبر دعامة للإعلان الوزاري الصادر في 20 ماي 1998.

وتسعى إلى مواصلة جدول الأعمال نفسه حول التجارة الإلكترونية، وأكدت أن الأعمال التي أقيمت إلى حد الآن والتي بينت أن التجارة الإلكترونية تعتبر تحديات جديدة من جهة ومعاملات تجارية جد مهمة لكافة الدول الأعضاء على كل مستويات التطور.

وتعترف بأهمية توفير والحفاظ على المحيط اللائق للتطوير المستقبلي للتجارة الإلكترونية، وقد تم الإعلان على أنه على الدول الأعضاء المحافظة على الممارسات الحالية والتي تترجم بعد فرض التعريفات الجمركية على التحويلات الإلكترونية إلى الدورة الخامسة[1]، ولقد أكدت على هذه التوصيات في الإعلان الوزاري الذي تم الاتفاق عليه في 18 ديسمبر 2005.

وكانت هذه الإعلانات ما هي إلاّ نتائج لمؤتمر جونيف الذي عقدته المنظمة العالمية للتجارة في ماي 1998، حيث تداول المؤتمرون موضوع التجارة الإلكترونية واتفقوا على وضع برنامج عمل يراعي الاحتياجات الاقتصادية والفنية للدول النامية إضافة إلى عدم فرض رسوم جمركية على الرسائل الإلكترونية، ريثما تكمل لجان المنظمة العلمية للتجارة دراسة برنامج العمل المشار إليه.

وقد تلخص موقف الدول المتقدمة وخاصة الولايات المتحدة الأمريكية في ضرورة خضوع المنتجات الإلكترونية لمبادئ المنظمة وتقنين عدم فرض الرسوم الجمركية على الرسائل الإلكترونية ريثما يتفق على هذا الإعفاء.

1- « Nous déclarons que les membres maintiendront leur pratique actuelle qui de na pas imposer de droits de douane sur les transmissions technologiques… » Voir : Conférence ministérielle de l'OMC, Doha 2001, Déclaration ministérielle, WT/MIN(01)/Dec1, 20 Novembre 2001, adoptée le 14 novembre 2001.

أما موقف الدول النامية فقد تمثل في:

- ضرورة استمرار التفاوض في الموضوعات الخاصة بالتجارة الإلكترونية ومتابعة دراستها في إطار مجالس المنظمة ولجانها المختصة، إذ أن هذا الموضوع يرتبط ارتباطا وثيقا باتفاقيات أخرى مثل تجارة الخدمات.
- أهمية توفير الدعم الفني والمالي للدول النامية لتمكينها من إنشاء بنية أساسية تؤهلها للمشاركة في التجارة الإلكترونية.
- العمل على تنفيذ الإعلان الوزاري الخاص بالتجارة الإلكترونية خاصة ما يتعلق منه بعدم فرض رسوم جمركية على الرسائل الإلكترونية إلى حين انعقاد المؤتمر الوزاري الرابع[1].

خامسا- الحماية من خلال المنظمة الدولية لضباط الجرائم المالية (IAFCI):

وهي منظمة دولية غير ربحية، تسعى لتوفير الخدمات وتوفير البيئة التي يمكن من خلالها جمع المعلومات حول الاحتيال الحالي وطرق التحقيق والحماية المالية، وقد تم إنشاء هذه المنظمة عام 1986 عن طريق التعاون بين 68 محققا دوليا مختصين في جرائم الأموال وتم من خلالها إنشاء منظمة دولية لضباط جرائم بطاقات الائتمان.

ومنذ 1992 تمنح هذه المنظمة عضويتها العادية لضباط الشرطة ومحققي مؤسسات إصدار البطاقات وخبراء مكافحة الاحتيال بشتى صوره، من خلال شروط خاصة بها وتتيح عضوية هذه المنظمة لأعضائها الحصول على المعلومات السرية الخاصة بالجرائم المالية الدولية والمجرمين الدوليين، وترسل إنذارات لأعضائها بالأماكن

---

[1]- وثيقة المؤتمر الوزاري الثاني للمنظمة العالمية للتجارة، جنيف، 18 ماي 1998، http://www.moqatel.com/openshare.behoth/ektesad8/wto/sec10.doc_cvt.htm .

- في 1917 تم الوصول إلى اتفاقية بخصوص خدمات الاتصالات السلكية واللاسلكية مع موافقة 69 حكومة على إجراءات تحريرية واسعة المدى تعدت تلك التي تم الاتفاق عليها في جولة الأروجواي، وفي نفس العام أتمت 40 حكومة بنجاح مفاوضات خاصة بدون تعريفات خاصة بمنتجات تكنولوجيا المعلومات، كما أتمت 70 من الدول الأعضاء اتفاقا خاصا بالخدمات المالية يغطي أكثر من 95% من التجارة البنكية والتأمين والأوراق المالية والمعلومات المالية، كما وافق أعضاء المنظمة العالمية للتجارة على الاجتماع الوزاري في ماي 1998 على دراسة مواضيع التجارة الناشئة من التجارة الإلكترونية العالمية. أنظر: . http://www.ar.wikipedia.org/wiki

المعرضة لهذه الجرائم، كما تتيح للعضو الدخول على شبكات الحاسب الآلي التي تخص الجرائم المالية.

فتقوم المنظمة بمكافحة جرائم واعتداءات بطاقات الائتمان، وتسعى أن يكون لديها وعي تام بالمنهج والطريقة التي يتبعها المحتالون، والعمل على جمع الاستخبارات على الأشخاص الذين يكون لهم نشاط في هذا المجال وفرض الحماية على المنتجات التي تصنع منها البطاقات وتحديد الأدوات المستخدمة في تنفيذ هذه الجرائم، حتى تتوفر للمنظمة الفرصة المبتكرة لردع ومواجهة هذه المخاطر[1].

[1]- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقة الائتمان، المرجع السابق، ص511.

خاتمـ ـ ـة

من خلال الدراسة التي تمت في إطار هذا البحث الذي يرتكز على التزام الدفع المهم جدا في مجال التجارة الإلكترونية، والمتمثل في الدفع الالكتروني الذي يتم على الخط (On line) بمناسبة عقد الكتروني أو عقد كلاسيكي إلاّ أن انقضاء التزام دفع ثمن السلعة أو الخدمة يمكن أن يتفق الأطراف على إتمامه بالطرق الحديثة. فالتقدم العلمي والتكنولوجي أحدث ثورة في المعاملات اليومية وذلك خدمة لمختلف المتعاملين الاقتصاديين المتدخلين في مجال نشاطاتهم.

فبعدما كانت الانترنت وليدة السباق نحو التسلح والذي يستعمل لأغراض عسكرية حيث تربط بين مختلف الإدارات العسكرية في الولايات المتحدة الأمريكية في سنوات الستينيات والسبعينيات، تم تحرير هذه الشبكة على باقي دول العالم بعد ذلك، والتي تعتبر شبكة الشبكات، ويظهر ذلك من خلال عموميتها وشموليتها، ويمكننا القول أنها الشبكة الأم، والتي تحتوي على الملايين من الشبكات المحدودة جغرافيا والتي تتصل بها بعقود اشتراك قصد تحقيقها للعالمية.

فتم تحليلها بعد ذلك لتشمل كم هائل من الخدمات التي توفرها مختلف هذه القنوات يتم تسخيرها للمعاملات الاقتصادية والتجارية وغيرها من المعاملات، يهدف استعمال هذه التكنولوجيا المتقدمة إلى ربح الوقت لامتيازها بسرعة المعاملات التي تتم عبر شبكات الاتصال وتقليل تكلفتها وكذلك هو الوضع بالنسبة للالتزام الذي يقع على عاتق الملتزم بالدفع والذي يعتبر شعاع التحليل والدراسة التي قمنا بها، فأصبحت العقود التجارية تتم عن طريق توصيل متعاملين بهذه الشبكة رغم بعدهم الجغرافي بعضهم البعض، ويتم ذلك بإرسال بيانات عبر شبكة الأنترنت بين أطراف العلاقة القانونية فترسل البيانات من الطرف الأول إلى الطرف الثاني، والثاني بدوره يرسل للطرف الأول ما يلزمه لإتمام العقد، فتكون المراسلة على شكل بيانات مجردة من الطابع المادي، من حاسوب الطرف الأول إلى الحاسوب الطرف الثاني، وهنا تظهر خاصية التجارة الإلكترونية، الأولى التجريد من طبيعتها المادية، وذلك لغياب الدعائم الورقية في المعاملات الإلكترونية.

وإذا كان انقضاء إلزام الدفع في العقد العادي في إطار التجارة العادية يتم بالشيك الورقي أو الكمبيالة الورقية أو الدفع المباشر للثمن، ففي ظل التجارة الإلكترونية تتم بوسائل مغايرة إلى حد كبير.

صحيح أن القواعد المنظمة لهذه الوسائل تبقى نفسها في ظل التجارة الإلكترونية باستثناء ميزة تجريدها من طابعها المادي وقواعد الإثبات التي نرجع إليها في حالة النزاع، فهي وسائل يتم معالجتها الكترونيا، أي عن طريق صورة الشيك أو الكمبيالة التي يتم معالجتهم الكترونيا، والتي ترسل على الخط لانقضاء الالتزام بين الأطراف، وتجدر الإشارة إلى أن تدخل وسيط بين متلقي الخدمة أو لسلعة والممول بها شيء لا مفر منه في التجارة الالكترونية ألا وهو البنك الذي يمكن أن يكون بنك تقليدي يوفر خدمات الدفع الالكتروني أو بنك الكتروني، والذي يكون للمتعاملين حسابات لديه، قصد إجراء المقاصة بين الحسابات مقابل عمولة وبدوره يشارك المتعاملين في التجارة الإلكترونية، بوضعه تحت تصرهم الوسائل التقنية قصد إتمام التزامات الأطراف منها نهائيات الدفع لموزعي الأوراق المالية، إلى جانب مواقع على الانترنت قصد الاستعلام حول الحسابات ...الخ.

فإذا كان الشيك الإلكتروني أو الكمبيالة المرقمة عبارة عن وسائل متطورة فقط بمعالجتها إلكترونيا، فقد ظهرت وسيلة حديثة وليدة التجارة الإلكترونية - ألا وهي البطاقات البنكية، وهي بطاقات بلاستيكية ذات مقاييس محددة عالميا تتخصص منظمات عالمية منها منظمة (Master card) و(Visa card) بإعطاء التراخيص للبنوك لإصدار مثل هذه الوسائل قصد التعامل بها بكل ما يخص الدفع الالكتروني.

الشيء الذي دفع إلى ضرورة وضع إطار قانوني ينظم هذه العلاقة الثلاثية بين مصدر البطاقة وحاملها والمتعامل الذي يقبل التعامل بها، والذي يعتبر مورد السلعة أو مقدم خدمة معينة، وذلك لأهمية المعاملات التي تتم بهذه الطرق التي تتداول بمناسبتها مبالغ ضخمة تحول عن طريقها من جهة الشيء الذي يعكس إقبال المجتمع على اقتنائها خاصة في المجتمعات الأوروبية وذلك تحقيقا للنجاعة والسرعة في المعاملات التي تتطلبها التجارة الالكترونية، فيقع على كل طر ف التزامات يتحملها وحقوق يتمتع بها وتحتوي هذه البطاقات البنكية رغم اختلاف أغراضها للدفع أو لسحب الأوراق...الخ، فهي

تحتوي على معلومات حاملها كالاسم واللقب، كما أن لها شريط مغناطيسي والذي يعبأ بمعلومات أو بيانات تمثل القيمة النقدية التي بحوزة حامل هذه البطاقة، فاعتمدت البنوك على الوسائل للحفاظ على زبائنها ولتسهيل تحويلاتهم المالية، وظهرت البنوك تتلاءم مع هذه التقنيات، وهي البنوك على الخط (E.Banking)، وهي عبارة عن مواقع على الويـ ب تقوم بهذه التحويلات الإلكترونية للأموال، كما ظهرت النقود الإلكترونية التي تعتبر على شكل بيانات تحتويها هذه الأشرطة المغناطيسية أو الشفرات المعبأة من طرف البنك الذي يضمن القيام بمختلف المقصاة التي تتيح استعمال هذه البطاقات في الأغراض المشروعة.

والجزائر ليست بمنأى عن هذه التطورات الاقتصادية، فبعدما كانت البداية محتشمة تقتصر على موزعات قليلة، وتقتصر على الجزائر العاصمة ظهرت بوادر أخرى كوضع نظام خاص ببطاقات لسحب الأوراق من الموزعين الأوتوماتيكيين من طرف بريد الجزائر، إلاّ أن حسب الإحصائيات يبقى الاستعمال المنتظر من هذه التقنية غير مقنع ويظهر ذلك من خلال الطوابير الطويلة في مراكز البريد.

وكذلك الاستعمال الكبير الشيكات الورقية لهذا الغرض إلى حد الآن، إلاّ أن البنوك التي استحدثت بطاقات البنكية خاصة بها مثل بنك التنمية الريفية، وكذلك بطاقة ما بين البنوك التي تقوم بغرض الدفع الإلكتروني التي تصدرها لزبائنها.

ويمكننا ملاحظة استعمال هذه الوسائل على مستوى الخطوط الجوية الجزائرية وكذلك بعض الصيدليات والمحلات التجارية الكبرى، إلا أن تعميم هذه الوسائل يبقى بعيدا عن ما هو منتظر مقارنة بالدول الأوروبية أو الدول المجاورة كتونس والمغرب.

ويمكن إرجاع ذلك إلى مستوى التقدم التكنولوجي والقانوني المتوسطين الذين تتمتع بهما الجزائر، وكذلك صعوبة تغيير عادة المواطن الجزائري وعدم ثقته في هذه الوسائل. فرغم أن هناك حماية تقنية للتعامل بهذه الوسائل لردع القرصنة الإلكترونية والسرقة ومختلف الاعتداءات التي تواجهها هذه الوسائل، عملت المؤسسات المتخصصة بالرقمية المعلوماتية، بوضع برامج ضمان وأمان قصد خلق الجو الملائم للتعامل بهذه الوسائل كبروتوكول SSL ومختلف تقنيات ردع كل أنواع القرصنة والاعتداءات غير المشروعة على الدفع الإلكتروني.

وقصد دعم ذلك كان من الضروري وضع تشريع ينظم هذه المعاملات المتعلقة أساسا بالتجارة الإلكترونية وبالدفع الإلكتروني خاصة لحساسية المعاملات الماليـة فأوجدت معظم الدول الأوروبية قوانين خاصة بالتجارة الإلكترونية وكذلك الدول العربية التي حذت نفس الحذو، قصد مسايرة عولمة التكنولوجيا والرقمية المفروضة، نتيجة للعولمة الاقتصادية.

كان الهدف من ذلك كسب أكبر جزء من السوق العالمية والتي تتعامل في ظل التجارة العالمية باستعمال التقنيات الإلكترونية. وما اهتمام الدول بضرورة تحقيق تعاون دول في هذا المجال إلاّ وعيا منها بأهمية هذه التقنيات ونجاعتها، وكذلك اهتمام المنظمات الدولية بها لوضع إطار قانوني اتفاقي ينظم هذه المعاملات التجارية الإلكترونية لدليل قاطع على ضرورة العمل والسعي قصد تحقيق النجاعة والتطور في مجال التجارة الإلكترونية وتحقيق تعاون دولي، والذي تسعى إليه منظمة التجارة العالمية وغيرها من المنظمات.

كما نستنتج أن الجزائر في طريقها إلى وضع نظام قانوني خاص بهذه المعاملات التجارية التي تتم عبر قنوات الاتصالات الحديثة،و يظهر ذلك من خلال القواعد القانونية التي نجدها في نصوص متفرقة والتي من الممكن أن تلعب دور فعال في وضع نظام قانوني إذا ما تم تجميعها في نص قانون موحد.

إلى جانب ذلك نستنتج انه يمكننا تصنيف هذا النظام القانوني للدفع الالكتروني واعتمادا على القانون المقارن يمكننا تصنيفه ضمن قانون الأعمال الذي وذلك لتجميعه للقانون التجاري وقانون الصرف وذلك للدور الأساسي الذي تلعبه البنوك لإتمام ولتطوير التزام الدفع بالطرق الالكترونية.

اعتمادا على ما سبق دراسته يمكننا وضع بعض الاقتراحات التي يمكن أن تساهم في تطوير هذه الوسائل في الجزائر لمواجهة العولمة وخاصة وأن الجزائر قد بادرت بالمفاوضات للانضمام إلى منظمة التجارة العالمية.

- ضرورة وضع تشريع خاص بالتجارة الإلكترونية بمختلف جوانبه قصد إعطاء ضمانات الاستعمال خاصة بالحماية القانونية للمتعاملين في مجال التجارة الإلكترونية، وعدم الاكتفاء ببعض المواد القانونية في نصوص متفرقة.
- فرض الاستفادة من تكوين الإطارات في مجال استعمال التكنولوجيا الرقمية في ظل تراخيص الاستثمار المخولة للبنوك الأجنبية التي تنشط في الجزائر مثل (Société Générale وBNP PARIBAS) للاستفادة من خبراتها وتجربتها.
- تحسيس المجتمع المدني بأهمية التعامل بهذه الوسائل الحديثة من خلال حملات ودراسات خاصة، قصد تهيئة البنية التحتية التي تتطور فيها التجارة الإلكترونية ويتحقق أساسا برفع المستوي الثقافي والمعرفي له.
- الاستفادة من تقنيات الأمان وبرامج الضمان التي تتطلبها هذه التقنيات وخاصة أن شركة ميكروسوفت لها وكالة في الجزائر قصد الاستفادة من خبراتها، ووضع شبكات لتأمين المعاملات المالية الإلكترونية.
- تسهيل إجراءات الحصول على بطاقات الدفع وتوفير تفتح الجميع على الانترنت قصد تطوير الوعي بهذا النوع من التجارة الطي يعتبر حتمية المستجدات الاقتصادية الراهنة. وبالتالي وضع إطار قانوني يشمل كافة الجوانب المتعلقة بهذا المجال من إصدار البطاقة إلى وضع إجراءات ردعية للمخاطر التي تمس بهذه التقنيات التي تجاب حتى المستثمرين الأجانب، لوجود تنظيم قانوني يحمي معاملاتهم وبيئة اقتصادية تضمن حسن سير معاملاتهم.
- يؤدي الأخذ بفكرة المستند الإلكتروني إلى ضرورة القيام بتعديلات في القوانين السارية المفعول في الدول، ويكون ذلك بالتعاون والتنسيق الدوليين في السياسات الجنائية. وذلك لتحقيق فعالية في مواجهة جريمة القرن ألا وهي الجريمة المعلوماتية التي تتعدى المفهوم التقليدي للحدود.

كما يجب العمل على توحيد المقاربات التي تقدم للمفاهيم في مجال التجارة الإلكترونية، كي لا تتستر هذه الأفعال وراء الفراغات القانونية أو اختلاف التكييفات

المقدمة لها للتحكم الفعال في ردع هذه الاعتداءات التي تمارس ضد المعاملات المالية الإلكترونية.

تظهر لنا تقنية الدفع الالكتروني من الناحية السطحية عملية بسيطة، إلاّ أنّها وما تم دراسته نستخلص أنّها يمكن أن تساهم في القضاء على الكثير من المشاكل التي تأثر على الاقتصاد الوطني، كالقضاء على مشكل نقص السيولة الذي تعاني منه الجزائر والتقليل إلى حد كبير من مشكل تزوير العملات النقدية و ذلك باستعمال النقود الالكترونية وتحقيقها للسرعة والأمان في المعاملات التجارية، كما يمكنها أن تساهم في إنجاح السياسة الاقتصادية للدولة في إطار المؤسسات الصغيرة والمتوسطة.

قائمة المراجع

أولا – المراجع باللغة العربية :

I- الكتب:

1. **محمد أمين احمد الشوابكه،** جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2004 .
2. **إبراهيم العيسوي**، التجارة الالكترونية، المكتبة الأكاديمية، الطبعة الأولى، مصر، 2003 .
3. **إبراهيم بختي،** التجارة الإلكترونية، مفاهيم واستراتيجيات التطبيق في المؤسسة، ديوان المطبوعات الجامعية، الجزائر، 2005.
4. **إيهاب فوزي السقا،** الحماية الجنائية والامنية لبطاقة الائتمان، دار الجامعة الجديدة، مصر، 2007 .
5. **بيارميل طوبيا،** بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، منشورات الحلبي الحقوقية، 2000 .
6. **جلال عايد الشورة ،** وسائل الدفع الالكتروني، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2008 .
7. **جمال زكي الجريدلي،** البيع الالكتروني للسلع المقلدة عبر شبكة الانترنت - دراسة فقهية مقارنة-، دار الفكر الجامعي، الطبعة الأولى، 2008 .
8. **حسن طاهر داود،** الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض.
9. **خالد ممدوح إبراهيم،** إبرام العقد الالكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006 .
10. **خالد ممدوح إبراهيم،** امن مراسلات البريد الالكتروني، الدار الجامعية، 2008 .

11. **رضا متولي وهدان**، النظام القانوني للعقد الإلكتروني والمسؤولية عن الاعتداءات الإلكترونية- دار الفكر والقانون، الطبعة الأولى، المنصورة، 2008.

12. **زياد سليم رمضان، محفوظ أحمد جودة**، الاتجاهات المعاصرة في ادارة البنوك، دار وائل للنشر والتوزيع، الطبعة الثانية، عمان، 2003 .

13. **سعودي محمد توفيق**، بطاقة الائتمان والأسس القانونية الناشئة عن استخدامها، دار الأمين للنشر، الطبعة الأولى، 2001،

14. **سمير حامد عبد العزيز الجمال**، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، الطبعة الأولى، القاهرة، 2006.

15. **شريف محمد غنام**، محفظة النقود الالكترونية – رؤية مستقبلية -، دار الجامعة الجديدة للنشر، مصر، 2007 .

16. **عبد الرحمن بن عبد ا السند**، الأحكام الفقهية للتعاملات الالكترونية، الحاسب الآلي وشبكة المعلومات، الانترنت، دار أبو راق للطباعة والنشر والتوزيع، الطبعة الأولى، 2004 .

17. **عبد الفتاح بيومي حجازي**، الجريمة في عصر العولمة، دار الفكر الجامعي، الطبعة الأولى، 2007 .

18. **عمر خالد زريقات**، عقود التجارة الالكترونية عقد البيع عبر الانترنت، دار الجامعة للنشر والتوزيع، الطبعة الأولى، 2007 .

19. **عمرو عيسى الفقي**، الجرائم المعلوماتية – جرئام الحاسب الآلي في مصر والدول العربية -، المكتب الجامعي الحديث، 2006 .

20. **فاروق محمد احمد الاباصيري**، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة الجديدة للنشر، 2002 .

21. **محمد أمين الرومي،** التعاقد الإلكتروني عبر الأنترنت، دار المطبوعات الجامعية، الطبعة الأولى، الإسكندرية، 2004.

22. **محمد بهجت عبد ا قايد،** الأوراق التجارية الالكترونية، دار النهضة العربية.

23. **محمد خليفة،** الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، 2007 .

24. **محمد دباس الحميد، ماركو إبراهيم نينو،** حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، الطبعة الأولى، عمان-الأردن، 2007 .

25. **محمد عبد حسين أل فرج الطائي،** المدخل إلى نظم المعلومات الإدارية – وائل للنشر والتوزيع، الطبعة الأولى، عمان-الأردن، 2005.

26. **محمد علي العريان،** الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004

27. **محمد عمر ذوابة،** عقد التحويل المصرفي الالكتروني، دار الثقافة للنشر والتوزيع الأردن، 2006

28. **مصطفى كمال طه،** وائل أنور بندق، الأوراق التجارية ووسائل الدفع الالكترونية، دار الفكر الجامعي، الإسكندرية، 2005.

29. **مصطفى محمد موسى،** أساليب إجرامية بالتقنية الرقمية - ماهيتها- مكافحتها- دراسة مقارنة، دار الكتب القانونية، 2005.

30. **ممدوح محمد خيري هاشم،** مشكلات البيع عن طريق الانترنت في القانون المدني -دراسة مقارنة -، دار النهضة العربية، 2000.

31. **منير الجنبيهي،** البنوك الالكترونية، دار الفكر الجامعي مصر، 2006 .

32. **نادر شعبان إبراهيم السواح،** النقود البلاستيكية وأثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، الدار الجامعية، 2006 .

33. **نضال إسماعيل برهم،** أحكام عقود التجارة الالكترونية، دار الثقافة للنشر والتوزيع الأردن، 2005 .

34. **وائل أنور بندق،** موسوعة القانون الالكتروني وتكنولوجيا الاتصالات، دار المطبوعات الجامعية، الإسكندرية، 2007 .

II .الرسائل و المذكرات العلمية:

1. **حابت أمال،** استغلال خدمات الانترنت، مذكرة لنيل درجة ماجستير في الحقوق فرع قانون الأعمال، جامعة مولود معمري، تيزي وزو، 2004.
2. **حمودي ناصر،** النظام القانوني لعقد البيع الدولي الالكتروني المبرم عبر الانترنت، رسالة لنيل درجة دكتوراه في القانون، جامعة مولود معمري، تيزي وزو، 2009.
3. **حميزي سيد أحمد،** تحديث وسائل الدفع كعنصر لتأهيل النظام المصرفي الجزائري، رسالة لنيل درجة ماجستير في العلوم الاقتصادية، فرع التحليل الاقتصادي، كلية العلوم الاقتصادية والعلوم التسيير، جامعة الجزائر، 2001.
4. **ركروك راضية،** البنوك وعمليات تبييض الأموال، مذكرة لنيل درجة ماجستير في القانون فرع قانون الأعمال، جامعة مولود معمري، تيزي وزو، 2006.
5. **عبد ا لبندة ،** النظام القانوني لبطاقة الدفع، مذكرة ماجستير في القانون الخاص – تخصص قانون الإصلاحات الاقتصادية -، جامعة جيجل، جيجل، 2007 .
6. **قرايش سامية،** التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية، مذكرة لنيل درجة الماجستير في القانون فرع "تحولات الدولة"، جامعة مولود معمري، 2009.
7. **الكاهنة إرزيل،** دور آلية تأمين القرض عند التصدير في التجارة الخارجية، رسالة لنيل درجة دكتوراه في العلوم تخصص القانون، جامعة مولود معمري، تيزي وزو، 2008.
8. **موكه عبد الكريم،** الثمن في عقود التجارة الدولية، مذكرة لنيل درجة ماجستير في القانون فرع قانون الأعمال، جامعة مولود معمري، تيزي وزو، 2007.

III. المقالات :

1. **قادري عبد المجيد ،** الوفاء الإلكتروني مجلة العلوم القانونية، جامعة باجي مختار عنابة، العدد12، جوان 2008، ص ص 168-169 .
2. **أسامة الكسواني،** التوقيع الإلكتروني، المجلة الإلكترونية، مقال منشور على الموقع الالكتروني: http://news.maktoub.com/article، ص3.
3. **أشرف توفيق شمس دين،** الحماية الجنائية للمستند الالكتروني، دراسة مقارنة، دراسة مقدمة في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، مركز البحوث والدراسات من 26 نيسيان إلى 28 نيسيان 2003، دبي، منشور على الموقع: http://www.lawjo.net
4. **أمجد جمالي،** حماية قواعد البيـانات وصلاحيات المستخـدمين، مـ ـقال منشور عـلى العنوان: www.arabteam2000-Forum.com، مجلة الفريق العربي، 2 أفريل 2005، ص1.
5. **أمجد حمدان الجهيني،** الاستخدامات الغير مشروعة لبطاقة الدفع الالكتروني من قبل الغير، مركز الدراسات القضائية، المملة الاردنية الهاشمية، مقال منشور على موقع : **www.coiss.com/replay.php**
6. **أمير حيدر،** حماية الدفع الإلكتروني؟ www.islamonline.net، 20-11-2004، ص01.
7. **أيمن قديح،** الدفع الالكتروني من يحميه؟ مقال منشور في: **http:/analysées.net.2006**
8. **بسمة رزق،** المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقة الدفع، بحث منشور على الموقع: http://www.mn940.net/forum، 28-06-2009، ص1.
9. **سالم الشاعر،** مقال منشور على الموقع، www.5alej.com/programs، 21-06-2009، ص 01.

10. **شريف محمد غنام،** محفظة النقود الإلكترونية، رؤية مستقبلية،بحث مقدم في مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي 10 و12 ماي 2003 ص 118. منشور على الموقع http://slconf.uaeu.acae

11. **عصمت سعد،** خسائرها بالمليارات ... جريمة الكترونية كل ثلاثة دقائق على الانترنت، 2008، مقال منشور على الموقع : www.ensan.net

12. **عماد يوسف حب ا** ، حماية الفضاء السبيراتي – الأمور التنظيمية لأمن المعلومات والاتصالات-، الهيئة المنظمة للاتصالات في لبنان: أمن الفضاء السبيراتي، 4-5 شباط 2009، مقال منشور على الموقع: http://www.tra.gov.lb/library

13. **محمد إبراهيم محمود الشافعي،** الآثار النقدية والاقتصادية والمالية للنقود الإلكترونية، بحث مقدم في مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي 10 و 12 ماي 2003 ص 140 منشور على الموقع http://slconf.uaeu.ac.ae

14. **محمد إبراهيم محمود الشافعي،** النقود الإلكترونية (ماهيتها، مخاطرها وتنظيمها القانوني)، مجلة الأمن والقانون، دبي، العدد الأول جانفي 2004، مقال منشور على الموقع http://www.mostathmr.com/vb/t12223.html

15. **محمد محرم محمد علي** ، جريمة النصب والتجارة الالكترونية ، مقال منشور على الموقع: www.f.law.net/law/index.php.2007

16. **محمود أحمد إبراهيم الشرقاوي،** مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون دبي 10 و12 ماي 2003 ص17. منشور على الموقع http://slconf.uaeu.au.

17. **هيثم عدنان عزو،** النقود الإلكترونية، مقال منشور على الموقع : http://www.arabe-law.com

IV.النصوص القانونية:

أ -النصوص الداخلية :

1. أمر رقم 66-156 مؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل و المتمم.
2. أمر 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية رقم 44 المؤرخة 2003/07/23.
3. أمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق ل 26 سبتمبر سنة 1975 المتضمن القانون المدني المعدل والمتمم بالقانون رقم 07-05 المؤرخ في 13 مايو سنة 2007.
4. أمر 2003-11 المؤرخ في 27 جمادي الثانية 1424 الموافق لـ 26 أوت 2003 المتضمن قانون النقد و القرض، الجريدة الرسمية رقم 52 المؤرخة في 27 أوت 2003.
5. قانون رقم 90-10 مؤرخ في 14 افريل 1990 المتعلق بالنقد والقرض جريدة رسمية عدد 16 مؤرخة في 18 افريل 1990 ملغى.
6. قانون 05-02 المؤرخ في 06 فيفري 2005 يعدل ويتمم الأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975 المتضمن القانون التجاري المعدل والمتمم.
7. قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها. الجريدة الرسمية عدد 47، 2009.
8. مرسوم التنفيذي رقم 2000-307 مؤرخ في 16 رجب عام 1421 الموافق 14 أكتوبر سنة 2000 يعدل المرسوم التنفيذي رقم 98-257 المؤرخ في 3 جمادي الأولى عام 1419 الموافق ل 25 غشت سنة 1998 الذي يضبط شروط وكيفيات إقامة خدمات أنترنات واستغلالها.
9. مرسوم تنفيذي رقم 05-442 مؤرخ في 12 شوال عام 1426 الموافق 14 نوفمبر 2005 يحدد الحد المطبق على عمليات الدفع التي يجب أن تتم بوسائل الدفع وعن طريق القنوات البنكية و المالية.الجريدة الرسمية العدد 75، 20 نوفمبر 2005.

10. مرسوم التنفيذي رقم 07-162 المؤرخ في 13 جمادي الأولى عام 1428 الموافق 30 مايو سنة 2007. يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 15 صفر عام 1422 الموافق 9 مايو سنة 2001، والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية. ج.ر العدد37، 2007.

11. تنظيم 97-03 المؤرخ في 16 رجب 1418 الموافق ل 17 نوفمبر 1997 المتعلق بغرفة المقاصة، الجريدة الرسمية رقم 17 المؤرخة في 25 مارس 1998.

ب- النصوص الدولية :

1. القانون النموذجي للتحويلات الدولية للأموال الصادر 12 أيار /مايو 1992 عن لجنة الأمم المتحدة لقانون التجارة الدولية.
2. القانون النموذجي بشان التجارة الالكترونية 1996 الصادر عن لجنة الأمم المتحدة لقانون التجارة الدولية، الجلسة العامة 85 المؤرخة في 16 كانون الأول/ديسمبر 1996. UNCITRAL المعدل سنة 1998.
3. اتفاقية المجلس الأوروبي الخاصة بالإجرام السبيري، بودابست، 23-11-2001، المواد 2-4 و7 منها.
4. اتفاقية الأمم المتحدة بشأن عقود البيع الدولي للبضائع المعتمدة في المؤتمر الدبلوماسي في 11 افريل 1980 والتي دخلت حيز النفاذ في 1 يناير 1988 منشورة على الموقع www.unicitral.org

V- وثائق أخرى:

1. **لجنة الأمم المتحدة للقانون التجاري الدولي،** الفريق العامل المعني بالتجارة الالكترونية، الجوانب القانونية من التجارة الالكترونية، الدورة 38 نيويورك، من 12-23 مارس 2001، ص3.
2. وثيقة المؤتمر الوزاري الثاني للمنظمة العالمية للتجارة، جنيف، 18 ماي 1998، http://www.moqatel.com/openshare.behoth/ektesad8/wto/sec10.doc_cvt.htm .

ثانيا- المراجع باللغة الفرنسية

I-OUVRAGES

1. **BOUKELLA M., BENABDALLAH (Y.), FERFERA (M.Y.)**, La méditerrané occidentale, entre régionalisation et mondialisation, édition CREAD, université Abderrahmane mira, Bejaïa, 2000.
2. **BRENDA Kieman**, E-commerce, stratégie α solutions, Microsoft presse, Paris, 2001.
3. **COMBORDE Christophe**, Sécurisez vos applications Internet (messagerie, Internet, site web, e-commerce), Éditions Dunod, Paris, 2004,
4. **ELIE Alfandari** , Droit des affaires les cadres généraux – **c ,** Litec , 1993 .
5. **ETIENNE Wery** , Facture monnaie et paiement électronique , Litec , 2003
6. **GAVALDA Ch., Michel E .**, Travaux diriges de droit des affaires - effet de commerce cheque est compte de crédit, Ed. Letic, Paris,1994.
7. **GAVALDA Ch., STOUFFLET J.,** Droit du crédit, effets de commerce chèques carte de paiement transfert de fonds, Ed. litec, 6eme édition, 2006,
8. **GAVALDA Ch.**, **STOUFFLET J.**, droit du crédit, effets de commerce, chèques, cartes de paiement et de crédit, édition litec, Paris , 2 ^{eme} édition, 1991.
9. **GRANIER Thierry** et **JOFFEUX Corynne**, Internet et transactions financières, Editions Economica, Paris, 2002,
10. **GROUMANN Sylvie Yettou,** Law foi électronique commerce, Thomson learing, 2000.
11. **JAMES T Perry et GARY P., Shneider,** E - commerce, Reynald goulet 2002.
12. **JEANTIN Michel,** Droit commercial: instruments de paiement et de Crédit entreprise en difficulté, 4ème éditions, 2005.
13. **JEANTIN Michel, PAUL Le Cannu**, Droit commercial: instruments de paiement et de Crédit, entreprise en difficulté, 5ème édition, Dalloz, Paris, 1999,

14. **JEFFREY F. Rayport Bernard J. Jaurorski**, Commerce électronique Traduit de l'américain par Francine Nézina Johanne champoux et Elisabéth Rochette, Edition Cheneliere/ McGram-Hill, Montréal – Toronto, 2003.
15. **MABROUK Hocine**, Code de la propriété intellectuelle, édition Houma, 1er édition , Alger, 2007
16. **MOUGENOT Dominique,** Droit des obligations, «la preuve», Édition larcier, 3 eme édition, Bruxelles ,2002.
17. **PEROCHON François**, Entreprises en difficultés Instruments de crédit et de paiement , LGDJ 4me Edition .
18. **PIEDELIEVRE Stéphane** , Instruments de crédit et de paiement , Dalloz, 3eme Edition, Paris, 2003.
19. **REGIS Bouyala,** Le monde de paiement, Edition revue banque, 2005.
20. **ROB Smith Mark Speaker et Mark Thomson**, comment faire votre commerce sur Internet , campus Press 2000
21. **ROGER Loroy Miller et Gaylord A.Jentz,** Law for Electronic, commerce, Thomson, 2000.
22. **SOLANGE Ghernaouti-Hélie,** Sécurité Internet – Stratégie et technologie, Éditions Dunod, 2000, Paris.
23. **TOERING Jean-Pierre et François Brion**, Les moyens de paiement, PUF, 1er Edition, 1999.
24. **TORTELLO Nicolle, LOINTIER Pascal,** Internet pour les juristes**,** Dalloz Delta, 1996.
25. **VOLLE Michel**, Economie des Nouvelles Technologie Internet**,** Edition Economica, Paris, 1994.

II-THESES ET MEMOIRES :

1. **YESSAD Houria**, le contrat de vente internationale de marchandises, thèse pour le doctorat en droit, université mouloud Mammeri de Tizi-Ouzou 2008.

2. **AIT OUAZZOU Zaina**, l'étendue de l'indépendance de la banque d'Algérie, mémoire pour l'obtention du magister en droit option droit des affaires, université mouloud Mammeri Tizi-Ouzou 2005.
3. **BINET Sophia**, l'utilisation des nouvelles technologies dans le procès civil, vers une procédure civile intégralement informatisée? mémoire master droit processuel, Université lumière Lyon2 voir : www.memoireonline.com
4. **BENCHOHRA Kara**, le commerce électronique en Algérie défis et perspectives, mémoire de fin d'étude pour l'obtention du diplôme d'ingénieur d'état en planification et statistiques, institut national de la planification et de la statistique, Alger, 2008.
5. **SENES Diane Et CLUZEAU Anna**, la cybercriminalité nouvelle enjeux de la protection des données, mémoire de fin d'étude, université Laval, lundi 15 décembre 2008.
6. **BENKADI Aissa, BELLADJEL Nassima, OUGHANEM Ali**, la monnaie électronique (une fonction d'avenir), mémoire de fin d'études en vue d'obtention d'une licence en sciences économique option: monnaie – finance-banque université Mouloud MAMMERI Tizi-Ouzou 2003.
7. **LAHOUAZI YOUCEF,** la monnaie électronique impacts et enjeux, mémoire de fin d'études, option techniques bancaires, université Mouloud MAMMERI Tizi-Ouzou 2003.
8. **Caroline BOISSEL, E-Greffe,** de la dématérialisation des actes de procédures vers le développement d'une justice en ligne? D.E.SS Droit et Pratique du commerce électronique, Université Paris V, Paris, 2004 in www.droit.univ-paris5.fr

IV-ARTICLES:

1. **Blanche Souzi,** - actualité européennes - revue des droit des affaires internationale, 1999.
2. **Brenda Kieman**, E-commerce, stratégie α solutions, Microsoft presse, France , 2001, p.250.
3. **Hubert de Vauplane**, le droit bancaire et la mondialisation des marchés financiers, R.J.C, le droit des affaires du XXI siècle, pp.187-204.

4. **Pascal Airault**, l'offensive des banques méditerranéennes, jeune Afrique, no 2479 du 13 au 19 juillet 2008, Tunisie, p72.
5. **Schwerer François**, de la circulation électronique de monnaie scripturale a la monnaie électronique universelle, Revue juridique commercial, Paris, 2001, pp55-64.
6. **Souzi Blanche**, Actualité européennes Revue de droit des affaires international, N° 2, 1999.
7. **Abdul Aziz Dia**, banque pour tous à l'horizon 2020. In www.afriqueblogue.com. Le 16 septembre 2009.
8. **Bonnaissa Karim**, le commerce et la vague Internet**,** mémoire de Licence en Management faculté des sciences de gestion, Laghouat : Algérie, in www.mémoireonline.com
9. **Caroline Riet,** Étude comparée des législations françaises et allemande, http://m2bde.u-paris10.fr, 23 juin 2008, p5.
10. **Dadjo Cica Mathilda,** Le contrats dans le cyberspace a l'épreuve de la théorie Générale, problème et perspective mémoire de maîtrise au droit des affaires et carriers juridique in www.mémoireonline.com
11. **Francis Lorentz**, commerce électronique, une nouvelle donnée pour les consommateurs, les entreprises, les citoyens et les pouvoirs public, in : http://www.minefi.gouv.fr/fond_documentaire/, p7.
12. **Gilles Mowas**, La sécurité des données dans les banques : enjeux et compétence, Éditions Jeudi mag, in : www.lesjeudis.com/magasineinformatique, publié le 24-09-2007
13. Mireille Antoine, La directive européenne sur la signature électronique : vers la sécurisation des transactions sur Internet? www.droit-technologie.org, 5-10-2000, p2 et 5.
14. **Myriam Berber**, une fraude aux faux cheque de banque, article publier sur : www.rfi.fr/actufs/articles/065/article-36301.asp
15. **Olivier Rimmel**, en 2004 la fraude a la carte bancaire sur internet augmente toujours en Europe, 7 février 2005. In : http// :www.epaysecurity.com
16. **Pierre Paul Lemyre**, Le guide juridique du commerce électronique in www.juristint.org, 02 06, 2009.

17. **Riet Caroline,** article 1108-1 du code civil français : « lorsqu'un écrit exige pour la validité d'un acte juridique, il peut être établi et conserve sous forme électronique », voir : http://m2bde.u-paris10.fr, 23 juin 2008, p.05.
18. **Steven J. Murdoch et Ross Anderson**, vérifié par visa et master card Secure code, étude du laboratoire informatique, université de Cambridge, royaume uni, in : http://www.cl.cam.uk/users/. P2.

V-AUTRES DOCUMENTS :

1. BADR Info, Revue bimestrielle d'information, N° 33, Mars-Avril, 2003.
2. Conférence ministérielle de l'OMC, Doha 2001, Déclaration ministérielle, WT/MIN(01)/Dec1, 20 Novembre 2001, adoptée le 14 novembre 2001.
3. contrat d'adhèrent de la Banque de Développement Local (BDL).
4. Déclaration de **GUESSOUM Fouzia**, In www.jeuneindipendant.com, jeudi 5 Mai 2005.
5. Document du service des études juridiques du senat (RF), La sécurité des transactions réalisées par carte bancaire, in :http://www.senat.fr/lc/lc125.html, Octobre 2003,
6. Jeune Afrique, hebdomadaire international indépendant, édition générale, Togo, no 2479 du 13 au 19 juillet 2008.
7. Le petit Larousse illustré, Paris, 2005.
8. Le petit robert 1, Paris, 1990.
9. Recommandation 87/598/CEE de la Commission Européenne du 8-12-1987 portant sur un Code Européen de bonne conduite en matière de paiement électronique, JOL 365, 24-12-1987.
10. Revue BADR Info Bimestrielle d'information N° 42, Mai/Juin, 2006.
11. **T.H**, le projet de certification électronique n'a toujours pas abouti, malaise à l'ARPT. Article, le soir d'Algérie, quotidien indépendant, dimanche 06/06/2010.

VI- SITE INTERNET:

1. http:// moqatel.com/openshare.behoth/ektesad8/wto/sec10.doc_cvt.htm
2. http://ar.wikipedia.org/wiki
3. http://dahnet.2005
4. http://droit-finance-commentcamarche.net/legifrance/37-codepenal
5. http://europa.eu/legislation-séminaire/international.
6. http://senat.fr/lc/lc125.html
7. www.balnet.net,
8. www.banquecentral.gov.sy/archive
9. www.commentaçamarche.net
10. www.wikipedia.org/wiki/cartdepaiement.



Caisse Nationale d'Epargne et de Prévoyance.
CNEP-Banque, « Société Par Actions » au capital social de 14.000.000.000,00 DA
Siège Social : 42, Rue Khelifa Boukhalfa. Alger



CONTRAT
CARTE INTERBANCAIRE DE PAIEMENT

Agence: *Code :*

Je soussigné(e):

Adresse: AIT ZAIM MAATKAS

Titulaire du compte N°(RIB) :

Déclare avoir reçu (e) une carte de type : CLASSIC

N° du contrat :

N° carte :

Avec les plafonds suivants :

Retrait : 000005500.00

Paiement : *ON_LINE :* 000009500.00 *OFF_LINE :* 000003500.00

Et pris connaissance des termes du présent contrat et y adhère complètement.

LES PARTIES ONT CONVENU DE CE QUI SUIT :

Article 1er : Objet du contrat
Le présent contrat a pour objet de fixer l'ensemble des conditions de délivrance, d'utilisation, de renouvellement, de mise en opposition et de retrait de la carte bancaire « CIB ».

Article 2 : Délivrance de la carte
La carte CIB est délivrée par la banque, dont elle reste la propriété, à la demande et sous réserve d'acceptation de cette demande, à ses clients titulaires d'un compte et/ou à leurs mandataires dûment habilités.
Le titulaire de la carte s'engage à utiliser la carte et/ou son numéro, exclusivement dans le cadre du Réseau Monétique Interbancaire (RMI) et des réseaux agréés.
La carte est rigoureusement personnelle, son titulaire devant y apposer obligatoirement sa signature dès réception. Il est strictement interdit au titulaire de la carte de la prêter ou de s'en déposséder Son usage est strictement limité aux opérations suivantes :

- retrait d'espèces dans les Distributeurs Automatiques de Billets (DAB) et les Guichets Automatiques de Banque (GAB),
- ordre de paiement pour régler l'achat d'un bien ou d'un service réellement effectué, au moyen des Terminaux de Paiement Electroniques (TPE).

En cas de changement d'adresse, le porteur de la carte, qu'il soit ou non le titulaire du compte sur lequel fonctionne celle-ci, doit en informer la banque.

Article 3 : Code confidentiel
Un code personnel est communiqué confidentiellement par la banque au titulaire de carte et uniquement à celui-ci. Le titulaire de la carte doit prendre toutes les mesures propres à assurer la sécurité de sa carte et du code confidentiel, il doit donc tenir absolument secret son code et ne pas le communiquer à qui que ce soit.
Le nombre d'essais successifs de composition du code confidentiel est limité à cinq (5) sur les appareils automatiques, avec le risque notamment de confiscation ou d'invalidation de la carte au 5ème essai infructueux.
La composition du code secret au niveau du DAB/GAB ou du TPE équivaut à une signature emportant reconnaissance de l'opération effectuée par le titulaire de la carte au moyen de celle-ci.

Article 4 : Modalités d'utilisation de la carte pour des retraits d'espèces dans les DAB/GAB et auprès des agences bancaires
4.1 - Les retraits d'espèces sont possibles dans les limites des montants plafonds hebdomadaires de retrait fixés dans les conditions de banque.
Les montants plafonds de retrait peuvent être différents selon que les transactions sont effectuées :
- sur les DAB/GAB de la banque ou sur ceux des autres banques et établissements financiers, auprès des
- guichets de la banque ou auprès de ceux des autres banques et établissements financiers.

4.2 - Les retraits d'espèces auprès des guichets sont possibles dans les limites des disponibilités du guichet payeur et sur présentation d'une pièce d'identité.
4.3 - Les montants enregistrés de ces retraits, ainsi que les commissions éventuelles, sont portés dans les délais habituels propres aux retraits d'espèces au débit du compte concerné sans aucune obligation d'indiquer le numéro ou le titulaire de la carte utilisée, notamment lorsque plusieurs cartes fonctionnent sur le même compte.
4.4 - Le titulaire du compte doit, préalablement à chaque retrait et sous sa responsabilité, s'assurer de l'existence au compte d'un solde suffisant et disponible et le maintenir jusqu'au débit correspondant.

Article 5 : Modalités d'utilisation de la carte pour le règlement d'achats de biens et de prestations de services
5.1- La carte est également un moyen de paiement qui peut être utilisé pour régler des achats de biens et des prestations de services.
5.2 - Ces paiements sont possibles dans les limites des montants plafonds mensuels de paiement fixés par la banque dans les conditions de banque.
5.3 - Les paiements par carte sont effectués selon les conditions et procédures en vigueur chez les Commerçants adhérant au Réseau Monétique Interbancaire et affichant le logo « CIB ».
5.4 - La banque a la faculté de débiter immédiatement le compte du montant des dépenses effectuées à l'aide de la carte en cas de décès, d'incapacité juridique du titulaire de la carte et/ou du titulaire du compte, d'incidents de paiement ou de fonctionnement du compte, de clôture du compte ou du retrait de la carte par la banque, décision qui serait notifiée au titulaire de la carte et/ou du compte par simple lettre.
5.5 - Le titulaire du compte autorise la banque à débiter son compte sur le vu des enregistrements ou des relevés transmis par le Commerçant, pour le règlement des achats de biens ou des prestations de services.
Les réclamations concernant ces opérations sont traitées dans les conditions prévues à l'article 16 « réclamations - conservation des documents et informations » ci-dessous.
5.6 - Le titulaire du compte doit s'assurer que le compte présente un solde suffisant et disponible, pour faire face à ses transactions de paiement.
5.7- Le montant détaillé des paiements par carte passés au débit du compte figure sur un relevé des opérations envoyé périodiquement au titulaire du compte, conformément aux conditions prévues par la convention d'ouverture de compte et/ou les conditions générales de banque.
5.8 - La banque reste étrangère à tout différend de nature commerciale, c'est à dire ne portant pas sur l'opération de paiement proprement dite, pouvant survenir entre le titulaire de la carte et le Commerçant.
L'existence d'un tel différend ne peut en aucun cas justifier le refus du titulaire de la carte et/ou du titulaire du compte sur lequel elle fonctionne, d'honorer les règlements par carte des achats de biens et des prestations de services.
5.9 - La restitution d'un bien ou d'un service réglé par carte bancaire ne peut faire l'objet d'une demande de remboursement auprès du Commerçant que s'il y a eu préalablement une transaction débitée d'un montant supérieur ou égal. Ce remboursement ne peut être qu'à l'initiative du Commerçant.

Article 6: Limitation et cessation de l'usage électronique de la carte
La banque, le titulaire du compte et le titulaire de la carte peuvent mettre fin à l'utilisation de celle-ci sans préavis ni justification.
De même, ils peuvent exclure du champ d'utilisation de la carte un ou plusieurs service(s) lié(s) à celle-ci ou supprimer l'accès à certaines fonctions du Réseau Monétique Interbancaire.
Toute limitation ou cessation de l'usage électronique d'une carte, à l'initiative de son titulaire ou du titulaire du compte sur lequel elle fonctionne, doit être notifiée par écrit à la banque qui s'efforcera d'en tenir compte dès réception.
La cessation de l'utilisation de la carte n'est opposable à la banque que si la carte lui a été restituée contre accusé de réception.

Article 7 : Preuve des opérations
Les opérations effectuées au moyen de la carte sont enregistrées automatiquement sur un support électronique. Ces enregistrements constituent la preuve des opérations effectuées au moyen de la carte et la justification de leur imputation au compte sur lequel cette carte fonctionne.
La banque, le titulaire du compte et le titulaire de la carte reconnaissent force probante au support informatique, sur lequel sont enregistrées les données relatives à toutes les opérations du Distributeur Automatique de Billets, du Guichet Automatique de Banque ou du Terminal de Paiement Electronique.

Article 8: Responsabilité de la banque
La banque n'est responsable des pertes directes encourues par le titulaire de la carte dues au dysfonctionnement du système que lorsque ce dernier incombe directement à la banque et n'est pas indépendant de sa volonté.
De même, la responsabilité de la banque est dégagée si le défaut est signalé au titulaire de la carte par un message sur l'appareil ou d'une autre manière visible.

Article 9 : Indisponibilité du système
La banque n'est nullement responsable des conséquences directes ou indirectes de l'inutilisation de la carte en cas d'indisponibilité technique du système.
L'indisponibilité du système est signalée par les DAB/GAB et les TPE.

Article 10: Recevabilité des oppositions
L'ordre de paiement donné au moyen de la carte est irrévocable. Seules sont recevables par la banque les oppositions, émanant du titulaire du compte et/ou de la carte, expressément motivées par la perte ou le vol de la carte, l'utilisation frauduleuse de la carte ou des données liées à son utilisation, le redressement ou la liquidation judiciaire du bénéficiaire du paiement.
L'opposition pour utilisation frauduleuse de la carte ou des données liées à son utilisation peut être effectuée dans le cas où le titulaire de la carte est toujours en possession de sa carte au moment de l'opération contestée uniquement dans les cas suivants :
- si la carte a été contrefaite,

- si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de la carte, avec son seul numéro et d'autres données y figurant.

Article 11 : Modalités de blocage et d'opposition de la carte

11.1- Le titulaire de la carte et/ou du compte doit déclarer immédiatement la perte ou le vol de la carte.
Cette déclaration doit être faite, pour le blocage de la carte, au Centre d'appel ouvert sept (7) jours par semaine, en appelant l'un des numéros de téléphone réservés à cet effet.
Un numéro d'enregistrement de ce blocage est communiqué au titulaire de la carte et/ou du compte.

11.2 - La banque ne saurait être tenue pour responsable des conséquences du blocage de la carte par téléphone qui n'émanerait pas du titulaire du compte.

11.3- Toute opposition doit être notifiée par le titulaire du compte ou le titulaire de la **carte à la** banque par lettre remise ou expédiée sous pli recommandé, à l'agence tenant le compte sur lequel fonctionne la carte, contre accusé de réception.
En cas de contestation sur l'opposition, celle-ci sera réputée avoir été effectuée à la date de la réception de ladite lettre par la banque.

11.4 En cas d'utilisation frauduleuse de la carte ou des données liées à son utilisation, le titulaire de la carte et/ou du compte doit faire opposition pour ce motif et la déclarer dans le délai prévu à l'article 16 « réclamations - conservation des documents et informations » ci-dessous.

11.5 - En cas de perte, de vol ou d'utilisation frauduleuse de la carte ou des données liées à son utilisation, la banque peut demander un récépissé ou une copie d'un dépôt de plainte ou de déclaration de perte faite aux autorités judiciaires.

Article 12 : Responsabilité du titulaire du compte

12.1 - Principe
Le titulaire de la carte est responsable de l'utilisation et de la conservation de celle-ci et de son code confidentiel.
Il assume, comme indiqué à l'article 12.2 «Opérations effectuées avant opposition» ci-dessous, les conséquences de l'utilisation de la carte tant qu'il n'a pas fait opposition dans les conditions prévues aux articles 10 « recevabilité des oppositions » et 11 « modalités de blocage et d'opposition de la carte » ci-dessus.

12.2 - Opérations effectuées avant opposition
Les opérations effectuées avant opposition sont à la charge du titulaire du compte, en cas de perte ou de vol de celle-ci.

12.3 - Opérations effectuées après opposition
Les opérations effectuées après opposition, dûment notifiée dans les conditions prévues à l'article 11 « Modalités de blocage et d'opposition de la carte » ci-dessus sont à la charge de la banque, à l'exception des opérations effectuées par le titulaire de la carte.

12.4 - Frais d'opposition
Les frais pour la mise en opposition de la carte bancaire sont supportés par le titulaire du compte suivant les conditions de banque en vigueur et les modalités fixées par la banque.

Article 13 : Responsabilité solidaire du ou des titulaires du compte et des cartes

En cas de compte joint, les titulaires du compte, lorsqu'ils ne sont pas titulaires de la carte, sont solidairement et indivisiblement tenus des conséquences financières résultant de la responsabilité du titulaire de la carte au titre de la conservation et de l'utilisation de la carte et du code confidentiel.
Cette responsabilité pèse sur les titulaires du compte jusqu'à ;

- la restitution de la carte à la banque et, au plus tard, jusqu'à la date de fin de validité, en cas de révocation, par le titulaire du compte, du mandat donné au titulaire de la carte ou la date de clôture du compte,
- ou la dénonciation de la convention de compte joint, à la condition que celle-ci ait été notifiée à tous les intéressés.

Les titulaires du compte doivent veiller à ce que leur compte présente un solde suffisant et disponible.

Article 14 : Durée de validité - Renouvellement - Retrait - Restitution de la carte

14.1 - La carte comporte une durée de validité dont l'échéance est inscrite sur la carte elle-même.

14.2 - A la date d'échéance, la carte fait l'objet d'un renouvellement automatique du support, sauf avis contraire exprimé par écrit avec accusé de réception par son titulaire ou le titulaire du compte concerné, au moins deux mois avant cette date,

14.3 - La banque a le droit de retirer, de faire retirer ou de bloquer l'usage de la carte à tout moment ou de ne pas la renouveler. La décision de retrait est notifiée dans tous les cas au titulaire de la carte et/ou du compte.
Le titulaire de la carte s'oblige, en conséquence, à la restituer à la première demande et s'expose à des sanctions si après notification du retrait de la carte, par simple lettre, il continue à en faire usage.

14.4 - La carte peut faire l'objet d'un retrait par un Commerçant ou par un établissement financier tiers, sur demande de la banque émettrice. Dans ce cas, la décision de restitution de la carte à son titulaire appartient à la banque.

14.5 - La clôture du compte sur lequel fonctionne une ou plusieurs cartes entraîne l'obligation de les restituer. Il en va de même en cas de dénonciation de la convention de compte collectif. L'arrêté définitif du compte ne pourra intervenir au plus tôt qu'un (1) mois après restitution des cartes.

Article 15: Capture de la carte

Une carte capturée par un DAB/GAB peut être récupérée par son titulaire au plus tard deux (2) jours après sa capture au guichet où est situé l'appareil, après accord du Centre d'autorisation de la banque. Passé ce délai, la carte est retournée à l'agence de la banque tenant le compte sur lequel fonctionne la carte.

Article 16 : Réclamations - Conservation des documents et informations

Le titulaire du compte et/ou de la carte a la possibilité de déposer une réclamation auprès de son agence, en présentant le ticket de l'opération litigieuse et l'extrait de compte, et cela dans un délai de quatre vingt dix (90) jours au maximum, à compter de la date de l'opération contestée.
Le ticket émis par le commerçant doit être conservé par le titulaire de la carte jusqu'à expiration du délai de réclamation.
Les informations ou documents ou leur reproduction que la banque détient, relatifs aux opérations visées dans le présent contrat et qui font l'objet de réclamation, doivent être produits par la banque quarante cinq (45) jours au plus après la réclamation du titulaire de la carte et/ou du compte.
La banque a l'obligation de faire diligence auprès de tout correspondant afin que celui-ci lui communique les pièces qu'il pourrait détenir et qui ont trait à l'opération contestée
Les parties conviennent d'apporter les meilleurs soins à leur information réciproque sur les conditions d'exécution de l'opération. Le cas échéant, et notamment en cas de fraude ou de suspicion de fraude commise par un tiers identifié ou non, la banque peut demander au titulaire de la carte un récépissé ou une copie d'un dépôt de plainte auprès des autorités judiciaires.

Article 17 : Remboursement en cas de réclamation

Les réclamations qui s'avèrent fondées conformément aux clauses de la présente convention donneront lieu au remboursement de tous les débits non justifiés, y compris la totalité des frais bancaires supportés le cas échéant par le titulaire du compte.
Le remboursement intervient au plus tard **soixante** (60) jours à compter de la réception de la réclamation

Article 18 : Communication de renseignements à des tiers

18.1 - De convention expresse, la banque est autorisée à diffuser les informations recueillies dans le cadre du présent **contrat**, les informations figurant sur la carte et celles relatives aux opérations effectuées au moyen de celle-ci aux banques et aux établissements financiers, aux organismes intervenant dans le cadre de la fabrication et du fonctionnement de la carte et éventuellement à des sous-traitants, aux commerçants acceptant le paiement par carte, ainsi qu'à la Banque d'Algérie et au Réseau Monétique Interbancaire.
Ces informations feront ou non l'objet de traitements automatisés, afin de permettre la fabrication de la carte, la gestion de son fonctionnement et d'assurer la sécurité des paiements notamment lorsque la carte est mise en opposition.

18.2 - Une inscription au fichier de la **centrale** des impayés, géré par la Banque d'Algérie, est réalisée lorsqu'une utilisation abusive de la carte par son titulaire ou le(s) titulaire(s) du compte est notifiée à ce(s) dernier(s)

18.3 - Le titulaire d'une carte peut exercer son droit d'accès aux données personnelles le concernant et demander à la banque la rectification de ces données, en cas d'erreur.

Article 19: Conditions tarifaires

19.1 - La carte est délivrée moyennant le paiement d'une cotisation annuelle dont le montant est fixé dans les conditions de banque. Cette cotisation est prélevée d'office sur le compte concerné
Dans le cas du renouvellement de la carte, tel que prévu à l'article 14 «durée de validité - renouvellement - retrait - restitution de la carte » ci-dessus, la cotisation est prélevée dans les mêmes conditions que lors de la délivrance de celle-ci.

19.2 - Une commission à l'opération est appliquée, notamment aux retraits d'espèces, aux mises en opposition pour perte ou vol de la carte, aux demandes de documentation et aux réclamations si ces dernières se révèlent non justifiées

19.3 - Les autres conditions tarifaires sont précisées dans le tableau des conditions de banque.

19.4 - Le titulaire du compte ou le titulaire de la carte peuvent obtenir auprès de toutes les agences de la banque la communication des tarifs pratiqués

19.5 - Le titulaire du compte autorise la banque à débiter son compte des cotisations et commissions visées ci-dessus.

Article 20 : Modification des conditions du contrat

La banque se réserve le droit d'apporter des modifications des tarifs, des plafonds hebdomadaires de retrait et des plafonds mensuels de paiement, qui seront portées à la connaissance du titulaire du compte.
Ces modifications sont applicables un mois après leur notification lorsqu'elles sont acceptées par le titulaire du compte.
En cas de non acceptation de ces modifications par le titulaire du compte, le présent contrat est résilié dans un délai d'un (1) mois à compter de la notification écrite du refus par le titulaire du compte ou de la carte

Article 21 : Sanctions

Tout usage abusif ou frauduleux, toute falsification de la carte, ainsi que toute fausse déclaration est passible des sanctions pénales prévues par la loi
Toute fausse déclaration ou usage abusif de la carte entraînent la résiliation du présent contrat.
Tous les frais et les dépenses réels engagés pour le recouvrement forcé des opérations résultant de l'utilisation de la carte sont à la charge solidairement du titulaire de la carte et du titulaire du compte concernés.
En cas d'indisponibilité de provision, la banque applique des pénalités, selon les conditions de banque en vigueur et les modalités fixées par la banque

Article 22 : Règlement des différends

22.1 - Hormis les litiges commerciaux, objet de la clause de l'article 5. alinéa 8 « modalités d'utilisation de la carte pour le règlement d'achats de biens et de prestations de services » ci-dessus, tous les litiges qui naissent à l'occasion de l'exécution ou de l'interprétation du présent contrat seront réglés à l'amiable
22.2 - A défaut de règlement amiable, les litiges seront soumis au tribunal compétent

Article 23: Résiliation du contrat

23.1- La résiliation du présent contrat intervient en cas de non exécution des obligations contractuelles par la banque, le titulaire du compte ou le titulaire de la carte
Toutefois, le titulaire de la carte ou du compte, d'une part, et la banque, d'autre part peuvent, a tout moment, sans justificatif ni préavis, sous réserve du dénouement des opérations en cours, mettre fin au présent contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité hormis l'envoi d'une lettre recommandée avec accusé de réception.
Lorsque cette résiliation fait suite à un désaccord sur les modifications des conditions du présent contrat, elle ne peut intervenir qu'au-delà du délai prévu dans l'article 20 « modification des conditions du contrat » pour l'entrée en vigueur de ces modifications.

23.2 - Tout décès et toute incapacité juridique du titulaire du compte ou de la carte entraînent la résiliation immédiate de plein droit du présent contrat, sous réserve du dénouement des opérations en cours Dans le cas où, après résiliation du contrat, il se révèlerait des impayes, ceux-ci seront à la charge du titulaire du compte.

23.3 - La résiliation prend effet au lendemain de la réception de la lettre recommandée ou avec accusé de réception.

23.4 - Les transactions antérieures à la résiliation seront traitées conformément aux conditions du présent contrat.

23.5 - La résiliation du présent contrat entraîne la restitution la carte à la banque par le titulaire du compte, contre accusé de réception.

Article 24 : Entrée en vigueur

Le présent contrat est établi en trois (3) exemplaires. Il entre en vigueur à compter de la date de sa signature par les parties.

Fait à Alger, le ____________

Signatures

P / la banque (écrire la mention manuscrite	**Le titulaire du compte** (écrire les mentions manuscrites « lu et approuvé »)	**Le titulaire de la carte** « lu et approuvé» et « bon pour acceptation de pouvoir »)

الفهـ ـ ـ ـرس

الفصل الثا : اطر الدفع الإلكترو وا ماية منها



ملخـ ـص

انقضاء الالتزام الدفع تصرف قانوني أساسي في العلاقات التجارية ،هذه الأخيرة التي تتطلب السرعة والائتمان بين المتعاملين الاقتصاديين.

أجابت على هذه المتطلبات التكنولوجيا الحديثة للمعلومات والاتصالات التي حملت في طيتها حلول لهؤلاء المتعاملين في إطار ما يسمى بالتجارة الإلكترونية.

توفر هذه الأخيرة وسائل تتلاءم وطبيعتها غير المادية، وذلك من خلال قنوات الاتصال و تبادل البيانات كالانترنت التي تسمح بنقل بيانات ذات قيمة مالية بالطرق الإلكترونية وذلك من خلال المعالجة الإلكترونية للبيانات. وكنتيجة لذلك ظهرت وسائل دفع إلكترونية كالشيك الإلكتروني والكمبيالة الممغنطة التي تفقد الطبيعة المادية التقليدية أكثر من ذلك اخترعت بطاقات بنكية معبأة بوحدات نقدية من طرف البنوك أو مؤسسات متخصصة في ذلك (Les Provider).

هذا التطور التكنولوجي الذي يخدم المتعاملين الاقتصاديين حمل في طيته عدة مخاطر تهدد المعاملات التجارية الإلكترونية خاصة التحويل الإلكتروني الأموال كالجريمة الإلكترونية التي تعيق تطور التجارة الإلكترونية، مما يستدعي إلى ضرورة مكافحتها بالوسائل التقنية والقانونية المسايرة للعصر الرقمي على المستويين الداخلي والدولي لتأمين وحماية هذه المعاملات التي تضمن السرعة والائتمان في التجارة الإلكترونية في عصر العولمة الرقمية المفروضة .

Résumé :

L'extinction de l'obligation du paiement est un acte juridique capital dans les transactions commerciales, ces dernières nécessitent la rapidité et la confiance entre les parties.

Les nouvelles technologies de l'information et de la communication apportent des solutions aux opérateurs économiques à travers le commerce électronique.

Ce E-commerce offre des moyens de paiement correspondant à la nature dématérialisée via les réseaux de transmission de données, tel que Internet, qui permet le transfert des fonds par les voies électronique en utilisant le traitement informatique des supports papier et la monnaie électronique émis par les provider.

Ce développement qui est aux services des opérateurs économiques porte en lui-même les risques de la cybercriminalité qui menacent la promotion du paiement électronique, d'où la nécessité d'une lutte technique et juridique effective, sur le plan national et international, pour la sécurisation de ces types de transactions et renforcer la confiance dans le commerce électronique qui assure la rapidité des transactions a l'ère de la mondialisation.